EXHIBIT A

SUPREME COURT OF THE STATE OF NEW YORK
COUNTY OF NEW YORK

----------X

Hiteks Solutions, Inc..

Plaintiff,

--against--

Citibank, N.A.; John Does 1-5; and
ABC Corporations 1-5;

Defendants.

----------X

Index No.:

Date Purchased: October 30, 2024

SUMMONS

Plaintiff designates New York County as the place of trial.

The basis of venue is CPLR 503 and because New York County is where a substantial part of events giving rise to claim occurred and is Plaintiff's place of business.

To Citibank, N.A.:

YOU ARE HEREBY SUMMONED to answer the complaint in this action and to serve a copy of your answer, or, if the complaint is not served with this summons, to serve a notice of appearance, on the attorneys for plaintiff within twenty (20) days after the service of this summons, exclusive of the day of service (or within thirty (30) days after the service is complete if this summons is not personally delivered to you within the State of New York); and in case of your failure to appear or answer, judgment will be taken against you by default for the relief demanded in the complaint.

Dated: New York, New York
October 30, 2024

SALZANO ETTINGER & LAMPERT LLP

By: _____

Jason Lampert, Esq.
104 West 40th Street, 14th Floor
New York, New York 10018
Tel: (212) 375-6746
Fax: (646) 365-3119
Attorneys for Plaintiff

TO: Citibank, N.A.
388 Greenwich Street
New York, New York 10013

New York Secretary of State
99 Washington Avenue
Albany, New York 12231

SUPREME COURT OF THE STATE OF NEW YORK
COUNTY OF NEW YORK
----------X

Hiteks Solutions, Inc.,

Plaintiff,

— against — **COMPLAINT**

Citibank, N.A.; John Does 1-5; and
ABC Corporations 1-5;

Defendants.
----------X

Plaintiff, Hiteks Solutions, Inc. ("Hiteks" or "Plaintiff"), by its attorneys Salzano Ettinger and Lampert LLP, and DeBenedictis & DeBenedictis LLC, alleges as follows:

NATURE OF THE ACTION

1. Hiteks is a health information technology ("IT") company that was founded in the State of New York in 2011. The company founder and Chief Executive Officer is Gerasimos Petratos.

2. Mr. Petratos, on behalf of Hiteks, first opened a business account with Defendant Citibank, N.A. (together with ABC Corporations 1-5 and John Does 1-5 hereinafter referred to as "Defendant(s)" or "Citibank") on or about 2013, opened a second account on or about 2017, and opened a third account on or about November 2023. Mr. Petratos is, and has been, the sole authorized user of the accounts.

3. On Friday, November 3, 2023, at approximately 3 p.m. ET, Mr. Petratos was in the New York office of Hiteks, and received a telephone call from someone who identified themselves as a representative from the Citibank Fraud Department.

4. The purported representative contacted Mr. Petratos at the authorized phone number for Hiteks's Citibank business account, and stated that Citibank had detected fraud on the Hiteks account. The representative knew that Mr. Petratos was the sole authorized user of the Hiteks account and knew the authorized phone number for the account.

5. The representative informed Mr. Petratos that there was a $600 charge at a Walmart in Texas that utilized the debit card associated with the Hiteks account, and asked him if it was a valid. Mr. Petratos told the representative that it was not. Based thereon, the representative told Mr. Petratos that they were going to freeze the card and lock the Hiteks bank account for two business days, to conduct a security breach investigation. The representative further told Mr. Petratos to check back in three business days to receive an update on Citibank's activity.

6. At no time did the representative ask Mr. Petratos for a password or other security information for the account. Nor did Mr. Petratos provide the representative with any security information or his account password.

7. Immediately thereafter—during the short period where Mr. Petratos believed that the Hiteks account was temporarily frozen for Citibank to investigate the alleged fraud—Citibank processed three unauthorized wire transfers from Hiteks's account. Each of the three wire transfers was purportedly for the purchase and/or renovation of real estate in three different states, and the money was sent to three named individuals of whom Hiteks had never sent a wire before.

8. The wire transfer special instructions for each request were sent in all capital letters, with several grammatical errors.

9. For the first wire transfer, which Citibank received on Monday, November 6, 2023 and processed that same day at 10:08 AM, Citibank wired $49,995.00 to Ashani Lewis ("Lewis"), who maintains an account with Wells Fargo Bank, N.A. ("Wells Fargo"), and whose address is in Hartford, Connecticut. *See* Exhibit A, Citi Wire Transfer Details. The "special instructions" for the wire transfer have zero relation to Hiteks's business. Specifically, the special instructions read: "NEED PAYMENT SENT URGENT BUSINESS DEAL CLOSING FOR RENOVATE AND REPAIRS." As is evident from even a cursory review of the wire transfer, the special instructions contain numerous grammatical errors. At no time has Hiteks ever used such language in a wire transfer request.

10. For the second wire transfer, which Citibank received on Tuesday, November 7, 2023 and processed that same day at 6:01 AM, Citibank wired $50,000.00 to Juliet Mendez ("Mendez"), who maintains an account with TD Bank, N.A. ("TD Bank"), and whose address is in Philadelphia, Pennsylvania. *See* Exhibit A, Citi Wire Transfer Details. The "special instructions" for the wire transfer have zero relation to Hiteks's business. Specifically, the special instructions read: "NEED PAYMENT SENT EXPEDITIOUSLY BUSINESS DEAL CLOSING TO RENOVATE."

11. For the third wire transfer, which Citibank received on Wednesday, November 8, 2023 and processed that same day at 6:01 AM, Citibank wired $49,999.89 to Lourdes Thalice Leon Fundora ("Fundora"), who maintains an account with Wells Fargo, and whose address is in Miami, Florida. *See* Exhibit A, Citi Wire Transfer Details. The "special instructions" for the wire transfer have zero relation to Hiteks's business. Specifically, the special instructions read: "NEED PAYMENT SENT EXPEDITIOUSLY FINALIZATION OF BUSINESS DEAL RENOVATIONS COMPLETED."

12. On November 8, 2023, Mr. Petratos attempted to access the Hiteks Citibank account only to realize that he was still locked out of the account.

13. He then contacted Citibank, and was connected with the Citibank Fraud Department. The Citibank representative told Mr. Petratos that, over the past three days, $149,994.89 was fraudulently wired to three individuals. The representative told Mr. Petratos to visit a Citibank branch and complete a fraudulent transaction form, and that the money would be credited bank to the Hiteks account. The Citibank representative also told Mr. Petratos that the third wire transfer, to Fundora, had not yet been finalized and that the representative would request that the wire transfer not be made. Despite these representations, Citibank failed to stop the third wire transfer from being sent from Hiteks's account.

14. Mr. Petratos visited a Citibank branch in Manhattan, and spoke with a branch supervisor, Joshua A. Carire. Mr. Carire holds the titles of Citibank Assistant Vice President and Citibank Retail Business Banker; his NMLS# is 1639769.

15. Mr. Carire told Mr. Petratos that he would need to notarize three affidavits that state he was not a party to the fraudulent transactions and that he did not authorize the fraudulent transactions. Mr. Petratos complied with this request. A copy of the notarized affidavits is attached hereto as Exhibit B.

16. Mr. Carire then told Mr. Petratos that Citibank would credit the money back to the Hiteks account, but that it might take a few months. In the meantime, Mr. Carire indicated that Citibank would permanently freeze the Hiteks account and that Mr. Petratos would have to open a new Hiteks business account, which he did.

17. Mr. Petratos also filed a complaint for stolen currency with the New York City Police Department. A copy of the police complaint is attached hereto as Exhibit C.

18. In follow-up discussions, both in-person at Citibank branches in New York and over the telephone with the Citibank Fraud Department, Citibank representatives repeatedly and consistently reassured Mr. Petratos that the money would be credited back to Hiteks. At no time did a Citibank representative say that there was a chance that the money would not be credited back to the Hiteks account.

19. Mr. Petratos kept in constant contact with Citibank regarding the refund, and repeatedly informed Citibank representatives that Hiteks was a small business and desperately needed that money to maintain payroll and for other business expenses.

20. For weeks—and then months—Citibank kept stalling, and then, without providing any explanation or evidence, told Mr. Petratos that he was at fault for the fraudulent wire transfers and that Citibank would not credit the Hiteks account. *See* Citibank Denial Letter, attached hereto as Exhibit D.

21. In turn, Hiteks was forced to obtain a short-term business loan to meet its payroll and business expenses. The short-term loan had an interest rate of 11.51%. For a loan of $199,000, Hiteks is obligated to repay, including interest, $257,700. A copy of the short-term loan is attached hereto as Exhibit E.

22. None of the three aforementioned wire transfers was initiated by Hiteks or an authorized user of Hiteks's account.

23. Each of the three aforementioned wire transfers was for business that bears no relation to Hiteks's business.

24. For each of the three aforementioned wire transfers, Citibank failed to authenticate the transfer through commercially reasonable means, despite the fact that the fraudulent wire

instructions specifically stated that the money was for business that bears no relation to Hiteks's business.

25. Moreover, at no time did Citibank's fraud department recognize the fraudulent activity on Hiteks's account over the three-day period in November 2023.

26. Defendant Citibank does not utilize commercially reasonable practices to detect fraud and prevent unauthorized wire transfers, nor does Citibank use commercially reasonable practices to notify customers in the event of fraud.

27. Citibank failed to accept the aforementioned wire transfer requests in good faith, and failed to comply with commercially reasonable security procedures, as required under the Uniform Commercial Code (U.C.C.) § 4-A-202(2).

28. Not using two-factor authentication is a commercially unreasonable security practice, known to Citibank.

29. The transfer notices themselves should have put Citibank on notice that the requested wire transfers were not typical transactions of Hiteks.

30. The transfer notices that Citibank processed used known fraudulent patterns of utilizing wire transfers of $50,000 or less.

31. These and other gaps and unreasonable practices in Citibank fraud protection policies and practices are well-documented, both in congressional testimony held on February 2, 2024 before the U.S. Senate Committee on Banking, Housing, and Urban Affairs (a copy of which is attached hereto as Exhibit F), and in a lawsuit that was filed against Citibank on January 30, 2024 by the Attorney General of the State of New York, a copy of which is attached hereto as Exhibit G.

32. While Citibank claims that Hiteks is solely responsible for the wire fraud, claiming that the wires were authenticated by Hiteks, see Exhibit D, Hiteks's insurance company has denied Hiteks's insurance claim, stating that there is no evidence that a malicious third party inappropriately accessed Hiteks's computer systems or its Citibank account credentials. These diametrically opposite positions cannot both be factually true. If Hiteks's computer systems or bank account details were breached by a malicious third party, Hiteks's insurance company likely is responsible for paying the insurance claim. If not, and Citibank's system was manipulated by a third party, then Citibank is responsible for refunding the wire transfers back to Hiteks. Moreover, even if Hitek's computer system or bank account details were breached, it does not absolve Citibank of its responsibility to maintain commercially reasonable security measures. That is, a malicious third party might have improperly gained access to Hiteks's Citibank account information, but was only able to request and receive three wire transfers because Citibank maintains lax and commercially unreasonable security measures.

33. Plaintiff Hiteks brings this Complaint against Defendant Citibank for violations of the U.C.C., conversion, fraud, and for violations of New York General Business Law Sections 349 and 350.

JURISDICTION AND VENUE

34. Jurisdiction and venue are proper in New York County because: Plaintiff Hiteks maintains an office in this district and opened a Citibank account in this District; Defendant Citibank owns, uses, or possesses property within New York County; the causes of action herein arise from Defendant Citibank's contracting with New York County residents and New York businesses to supply goods and services in New York County; and/or Defendant Citibank has

committed tortious acts within and without New York County causing injury to persons or property within New York County. N.Y. C.P.L.R 301; N.Y. C.P.L.R 302; N.Y. C.P.L.R 503.

THE PARTIES

35. Hiteks Solutions Inc. is a Delaware corporation that maintains an address at 447 Broadway, 2nd Floor, New York, New York 10013.

36. Defendant Citibank, N.A. is a national bank whose principal offerings include: investment banking, commercial banking, cash management, trade finance, and e-commerce; private banking products and services; consumer finance, credit cards, and mortgage lending; and retail banking and services. As of 2022, Citibank held more than $1 trillion in deposits, including more than $400 in consumer deposits. Defendant Citibank is headquartered at 5800 South Corporate Place, Sioux Falls, South Dakota 57108. Defendant Citibank is the wholly owned subsidiary of Citigroup, Inc., headquartered at 388 Greenwich Street, New York, New York 10013.

37. John Does 1-5 are individuals, not currently known to Plaintiff, who were responsible, in whole or part, for the Citibank's decision to not use two factor authentication, implement the misleading disclosures regarding Citibank's security procedures, mislead account holders as to the adequacy of Citibank's security procedures, and/or are responsible in whole or in part for the harms suffered by Plaintiff.

38. ABC Corporations 1-5 are corporate entities, affiliates, subsidiaries, and/or related entities to Citibank not currently known to Plaintiff, who were responsible, in whole or part, for the harms suffered by Plaintiff.

FACTUAL ALLEGATIONS

A. Citibank Processes Three Fraudulent Wire Transfers and Then Promises to Credit the Money Back to Hiteks's Bank Account

39. Hiteks incorporates the proceeding paragraphs as if set forth herein.

40. Hiteks is a health IT company that was founded in the State of New York in 2011. The company founder and Chief Executive Officer is Gerasimos Petratos. The company was incorporated in Delaware on or about 2017.

41. Mr. Petratos, on behalf of Hiteks, opened a business checking account with Citibank on or about on or about 2013, with a second account opened on or about 2017. Mr. Petratos is the sole authorized user of the account.

42. On Friday, November 3, 2023, at approximately 3 p.m. ET, Mr. Petratos was in the New York office of Hiteks, and received a telephone call from someone who identified themselves as a representative from the Citibank Fraud Department. The representative contacted Mr. Petratos at the authorized phone number for Hiteks' Citibank account, and stated that Citibank had detected fraud on the Hiteks bank account. The representative knew that Mr. Petratos was the sole authorized user of the Hiteks account and knew the authorized phone number for the account. At no time did the representative ask Mr. Petratos for a password or other security information for the account. Nor did Mr. Petratos provide the representative with any security information or his account password.

43. The representative told Mr. Petratos that there was a $600 charge at a Walmart in Texas that utilized the debit card associated with the Hiteks account, and asked him if it was a valid charge. Mr. Petratos told the representative that it was not a valid charge, and the representative told Mr. Petratos that they were going to freeze the card and lock the Hiteks bank

account for two business days. The representative then told Mr. Petratos to check back in three business days to receive an update on the activity.

44. Immediately thereafter, while Mr. Petratos believed that the Hiteks account was temporarily frozen for Citibank to investigate the alleged fraud, Citibank processed three unauthorized wire transfers from Hiteks's account. Each of the three wire transfers was purportedly for the purchase and/or renovation of real estate in three different states, and the money was sent to three named individuals of whom Hiteks had never sent a wire before.

45. For the first wire transfer, which Citibank received on Monday, November 6, 2023 and processed that same day at 10:08 AM, Citibank wired $49,995.00 to Ashani Lewis ("Lewis"), who maintains an account with Wells Fargo Bank, N.A. ("Wells Fargo"), and whose address is in Hartford, Connecticut. *See* Exhibit A, Citi Wire Transfer Details. The "special instructions" for the wire transfer have zero relation to Hiteks's business. Specifically, the special instructions read: "NEED PAYMENT SENT URGENT BUSINESS DEAL CLOSING FOR RENOVATE AND REPAIRS." As is evident from even a cursory review of the wire transfer, the special instructions contain numerous grammatical errors. Upon information and belief, Lewis maintains an address at 111 Woodlawn Circle East, Hartford, Connecticut 06108, and maintains an account, number 5797826822, with Wells Fargo.

46. For the second wire transfer, which Citibank received on Tuesday, November 7, 2023 and processed that same day at 6:01 AM, Citibank wired $50,000.00 to Juliet Mendez ("Mendez"), who maintains an account with TD Bank, N.A. ("TD Bank"), and whose address is in Philadelphia, Pennsylvania. *See* Exhibit A, Citi Wire Transfer Details. The "special instructions" for the wire transfer have zero relation to Hiteks's business. Specifically, the special instructions read: "NEED PAYMENT SENT EXPEDITIOUSLY BUSINESS DEAL CLOSING

TO RENOVATE." Upon information and belief, Mendez maintains an address at 4744 North Mascher Street, Philadelphia, Pennsylvania 19120, maintains an account, number 031101266, with TD Bank.

47. For the third wire transfer, which Citibank received on Wednesday, November 8, 2023 and processed that same day at 6:01 AM, Citibank wired $49,999.89 to Lourdes Thalice Leon Fundora ("Fundora"), who maintains an account with Wells Fargo, and whose address is in Miami, Florida. *See* Exhibit A, Citi Wire Transfer Details. The "special instructions" for the wire transfer have zero relation to Hiteks's business. Specifically, the special instructions read: "NEED PAYMENT SENT EXPEDITIOUSLY FINALIZATION OF BUSINESS DEAL RENOVATIONS COMPLETED." Upon information and belief, Fundora maintains an address at 630 SW 62nd Avenue, Miami, Florida 33144, and maintains an account, number 7466624868, with Wells Fargo.

48. On November 8, 2023, Mr. Petratos attempted to access the Hiteks Citibank bank account only to realize that he was still locked out of the account.

49. He then contacted Citibank, and was connected with the Citibank Fraud Department. The Citibank representative told Mr. Petratos that, over the past three days, $149,994.89 was fraudulently wired to three individuals. The representative told Mr. Petratos to visit a Citibank branch and complete a fraudulent transaction form, and that the money would be credited bank to the Hiteks account. The Citibank representative also told Mr. Petratos that the third wire transfer, to Fundora, had not yet been finalized and that the representative would request that the wire transfer not be made. Despite these representations, Citibank failed to stop the third wire transfer from being sent from Hiteks's account.

50. Mr. Petratos visited a Citibank branch in Manhattan, and spoke with a branch supervisor, Joshua A. Carire. Mr. Carire holds the titles of Citibank Assistant Vice President and Retail Business Banker. His NMLS# is 1639769.

51. Mr. Carire told Mr. Petratos that he would need to notarize three affidavits that state he was not a party to the fraudulent transactions and that he did not authorize the fraudulent transactions. *See* Exhibit B.

52. Mr. Carire then told Mr. Petratos that Citibank would credit the money back to the Hiteks account, but that it might take a few months. In the meantime, Mr. Carire indicated that Citibank would permanently freeze the Hiteks account and that Mr. Petratos would have to open a new Hiteks business account, which he did.

53. Mr. Petratos also filed a complaint for stolen currency with the New York City Police Department. *See* Exhibit C.

54. In follow-up discussions both in person at Citibank branches over the telephone with the Citibank Fraud Department, Citibank representatives repeatedly and consistently reassured Mr. Petratos that the money would be credited back to Hiteks. At no time did a Citibank representative say that there was a chance that the money would not be credited back to the Hiteks account.

55. Mr. Petratos kept in constant contact with Citibank regarding the refund, and repeatedly informed Citibank representatives that Hiteks was a small business and desperately needed that money to maintain payroll and other business expenses.

56. For weeks—and then months—Citibank kept stalling, and then told Mr. Petratos that he was at fault for the fraudulent wire transfers and that Citibank would not credit the Hiteks account. *See* Exhibit D.

57. In turn, Hiteks was forced to obtain a short-term business loan to meet its payroll and business expenses. The short-term loan had an interest rate of 11.51%. For a loan of $199,000, Hiteks is obligated to repay, including interest, $257,700. *See* Exhibit E.

B. Citibank Failed to Accept the Wire Transfer Requests in Good Faith and Failed to Comply with Commercially Reasonable Security Procedures

58. None of the three aforementioned wire transfers was initiated by Hiteks or an authorized user of Hiteks's account.

59. Each of the three aforementioned wire transfers was for business that bears no relation to Hiteks's business.

60. For each of the three aforementioned wire transfers, Citibank failed to authenticate the transfer despite the fact that instructions specifically state that the money was for business that bears no relation to Hiteks's business.

61. Moreover, at no time did Citibank's fraud department recognize the fraudulent activity on Hiteks's account over the three-day period in November 2023.

62. Defendant Citibank does not utilize commercially reasonable practices to detect fraud and prevent unauthorized wire transfers.

63. Citibank failed to accept the aforementioned wire transfer requests in good faith, and failed to comply with commercially reasonable security procedures, as required under U.C.C. § 4-A-202(2).

64. The transfer notices themselves should have put Citibank on notice that the requested wire transfer was not a typical transaction of Hiteks.

65. The transfer notices that Citibank processed used known fraudulent patterns of utilizing wire transfers of $50,000.00 or less.

66. These and other gaps and unreasonable practices in Citibank fraud protection policies and practices are well-documented.

67. A New York Attorney General investigation has revealed Citibank's widespread failure to use commercially reasonable security procedures.[1] *See* Exhibit G. As the complaint details: "Defendant Citi has not deployed sufficiently robust data security measures to protect consumer financial accounts, respond appropriately to red flags, or limit theft by scam. Instead, Citi has overpromised and underdelivered on security, reacted ineffectively to fraud alerts, misled consumers, and summarily denied their claims. Citi's illegal and deceptive practices have cost New Yorkers millions." *Id*. at p. 2.

68. Citibank's unreasonable security precautions are caused, in part from the following: Citibank has connected wire transfer services to an account holder's online and mobile banking and has adopted unreasonable security measures to stop scammers from infiltrating the accounts and making unauthorized wire transfers. *See, e.g., id*.

69. Citibank's unreasonable security measures include, but are not necessarily limited to, the following:

a. Citibank permits scammers to alter contact information, usernames, and passwords, upgrade accounts to access online wire transfer services, and consolidate funds across multiple accounts, all without subjecting to robust scrutiny scammers' subsequent requests to initiate large-dollar wire transfers that will empty consumers' accounts;

b. Citibank fails to employ tools that effectively monitor and respond to

[1] The complaint also provides copious details on how wire transfers are implemented in the U.S. banking system, see Exhibit G at pp. 11-16, and how Citibank employs unreasonable security measures to stop scammers. *See* Exhibit G at pp. 25-28.

anomalous consumer or account activity, such as wire transfers that are the first ever involving consumers' accounts, that are for out-of-the-ordinary amounts based on past activity, or that will effectively empty consumers' accounts; and

c. Even when alerted to fraudulent activity, Citibank does not effectively secure consumers' bank accounts, which remain vulnerable to scammers.

See, e.g., id. at p. 4.

70. Citibank has failed to develop, implement, and maintain reasonable safeguards to protect the security, confidentiality, and integrity of Hiteks's financial account information.

71. Citibank has failed to maintain a data security program that is appropriately designed to detect, prevent, and mitigate identify theft in response to red flags indicative of possible identity theft.

72. The U.C.C. generally provides that banks must reimburse customers for unauthorized Payment Orders. U.C.C. § 4-A-204(1). However, banks and their customers can agree upon specific security procedures for verifying Payment Orders that the banks receive. U.C.C. § 4-A-201. And if banks can prove that these procedures are commercially reasonable, were followed, and that Payment Orders were accepted in good faith, the UCC provides that the banks need not reimburse customers, even for unauthorized Payment Orders. U.C.C. § 4-A-203.

73. Whether particular security procedures are commercially reasonable is determined by a variety of factors, including the circumstances of the customer known to the bank, such as the size, type, and frequency of Payment Orders normally issued by the customer to the bank.

74. The U.C.C. specifies that use of an authorized signature specimen alone is not a

sufficient security procedure. Consistent with this approach, legal and policy consensus is that comparable single-factor procedures, such as an online username and password, also are not a commercially reasonable security procedures standing alone. For example, the Federal Financial Institutions Examination Council ("FFIEC"), a federal interagency body that prescribes uniform procedures for U.S. financial institutions, has publicly cautioned that use of single-factor authentication is inadequate either to safeguard against scammers fraudulently infiltrating customers' online or mobile banking or to prevent widespread payment fraud.

75. Multi-Factor Authentication ("MFA"), as opposed to single-factor authentication, is one available control for financial institutions to prevent fraudulent online or mobile activity. MFA requires more than one distinct authentication factor. The factors are something consumers know (such as usernames and passwords), something consumers have (such as mobile devices), and something consumers are (such as fingerprints or other biometric identifiers).

76. MFA, however, has been shown to be ineffective when used alone. Consumers' email accounts, browsers, and mobile devices are common access points for scammers. Thus, the FFIEC recommends that financial institutions employ layered security approaches, which incorporates multiple preventative, detective, and corrective controls, and which is designed to compensate for potential weaknesses in any one control, including MFA.

77. A critical aspect of layered security is an evaluation of consumers and their account histories, including usage patterns, the frequency of high-dollar transactions, and whether transactions or other recent online behaviors are anomalous. Nacha, the entity formerly known as the National Automated Clearinghouse Association, which manages the ACH payment network, has commented that commercially reasonable, risk-based approaches to security will consider

account characteristics and anomalous behavior. When banks identify anomalous behavior or transactions, commercially reasonable and effective controls will prompt the banks to employ more robust procedures to scrutinize and verify electronic payment activity.

78. In addition to MFA, layered security can include a number of other effective controls, such as requiring dual authorization through different access devices, such as a phone call to a landline and a text message to a mobile device, limits on transaction frequency or size based on prior usage patterns, and the use of enhanced authentication techniques after changes to account types or characteristics, such as account upgrades or changes to passwords.

79. Another aspect of effective layered security is sufficient training and controls for call center and fraud prevention employees. Scammers use engineering and other sophisticated techniques to deceive these employees into resetting passwords or granting scammers access to accounts, including online or mobile banking. Commercially reasonable security procedures are those that employ monitoring and processes to defeat fraudulent transactions in real time.

80. Plaintiff further alleges that Citibank has repeatedly and deceptively induced Hiteks to enter into agreement for banking services with Citibank setting forth inadequate security procedures, misleading Hiteks about its rights, depriving Hiteks of statutory safeguards, falsely promising Hiteks that its money is secure when it is not, tricking Hiteks into executing unnecessary affidavits, inflating the likelihood of recovery of stolen funds, and blaming Hiteks without reason or justification.

C. Citibank Has Engaged in False Advertising and Deceptive Business Practices

81. As detailed in this Complaint, Defendant Citibank has engaged in false advertising and deceptive business practices.

82. Citibank advertises to prospective business account clients that it provides "Security & Fraud Protection." Citibank further advertises: "Business Banking Made Easy." Even more, Citibank advertises that its security and fraud protection measures "Protect your business against losses from unauthorized activities in your Citibank accounts." *See* "Bank Accounts for Your Business," citi.com (accessed October 17, 2024).

83. Defendant Citibank further advertises: "Citi Protects You." Via Defendant Citibank's "Security Center," Defendant Citibank advertises that "From fraud to identity theft, our comprehensive suite of advanced security features and services help keep you protected."

84. With respect to fraud detection and warning alerts, Defendant Citibank further advertises: "Accounts routinely monitored to detect fraud or unauthorized use." Moreover, within this realm, Defendant Citibank advertises that it "will flag suspicious activity" and contact customers when suspicious activity occurs.

85. The aforementioned advertising and marketing statements of Defendant Citibank are false and/or misleading, because in fact Citibank does not provide commercially reasonable security and fraud detection measures for its banking customers.

86. Defendant Citibank also has engaged in deceptive business practices, in that it entices New York residents to open bank accounts by promising that it maintains commercially reasonable security and fraud detection measures.

87. Specifically, Defendant Citibank knowingly does not use commercially reasonable means to safeguard customer bank accounts, prevent unlawful access to customer bank accounts, detect fraud on customer bank accounts, process wire transfers for customer bank accounts, and contact customers in instances of suspected fraud on their bank account. These actions

88. Citibank also knowing, deliberately, and/or intentionally withheld these facts in an attempt to persuade Hiteks, and other customers, to agree that Citibank's practices were commercially reasonable. This too constitutes a deceptive business practice.

D. Defendant's Wrongful and Illegal Conduct has Damaged Hiteks

89. Defendant's wrongful and illegal conduct has damaged Hiteks.

90. Prior to the below signed counsel's involvement, Citibank has refused to credit the fraudulent transfer amount, $149,994.89, back to Hiteks's account, as the company repeatedly and consistently promised it would do.

91. This was despite the fact that Hiteks repeatedly informed Citibank that the company, as a small business, desperately needed the money for payroll and other business expenses.

92. Due to Defendants wrongful and illegal conduct, Hiteks has been damaged in the amount of $149,994.89, plus interest dating back to the dates of the unauthorized transfers in November 2023.

93. Since Citibank refused to credit the money, it was necessary for Hiteks to obtain a short-term loan to cover its payroll and business expenses. The short-term loan had an interest rate of 11.51%, and Hiteks is obligated to pay back $58,700 in interest. *See* Exhibit E.

94. The amount of $58,700 is further damage that Hiteks has suffered due to Defendants' wrongful and illegal conduct.

95. Hiteks has suffered further damage due to the interference with its business activities and the need to retain counsel to remedy the harms caused by Defendant in this matter.

96. Hiteks brings this Complaint against Defendant for violations of the U.C.C., conversion, fraud, and for violations of New York General Business Law Sections 349 and 350.

97. Defendants purposefully, deliberately, intentionally, and/or knowingly misrepresented and/or admitted material facts as to the adequacy and commercially reasonableness of its security practices for wire transfers.

98. For example, Defendants knew and/or were on imputed in and/or had actual notice that failure to use two factor authentication was a de facto commercially unreasonable security procedure, but hid this fact from account holders such as Hiteks.

FIRST CAUSE OF ACTION

Violations of the U.C.C.

Against Defendant Citibank

99. Plaintiff repeats and realleges each of the foregoing allegations as if fully and completely set forth herein.

100. The U.C.C. generally provides that banks must reimburse customers for unauthorized Payment Orders. U.C.C. § 4-A-204(1).

101. Under Article 4-A of the U.C.C., Citibank cannot refuse to refund payments for unauthorized Payment Orders unless Citibank accepted the Payment Orders in good faith and in compliance with commercially reasonable security procedures and any instructions of its customers restricting acceptance of payment orders. U.C.C. § 4-A-202(2).

102. Citibank has the burden of establishing that it is more probable than not that it acted in good faith and in compliance with the security procedures. U.C.C. § 4-A-105(g).

103. Under Article 4-A of the U.C.C., if Citibank determines that its customers' funds were stolen in connection with unauthorized Payment Orders that were not enforceable, Citibank "shall refund any payment . . . and shall pay interest on the refundable amount calculated from the date the bank received payment to the date of the refund." U.C.C. § 4-A-204(1).

104. Citibank has failed to employ commercially reasonable security procedures in connection with its handling of Payment Orders sent electronically via wire transfer requests in the following respects:

a. Citibank's online terms and conditions have incorporated single-factor authentication protocols to verify Payment Orders sent electronically instead of layered security, including MFA, algorithmic monitoring of consumer and account behavior, mechanisms to identify high-risk transactions or anomalous behavior that trigger strengthened procedures, transaction limitations based on frequency, volume, and repeat activity, and training to ensure effective real-time responses to potential fraud, all of which are the hallmarks of commercially reasonable security procedures;

b. Citibank has failed to materially alter and employ its most robust verification procedures and protocols in response to anomalous activity that should have indicated suspicious or fraudulent activity, including Payment Orders that: (i) were received within hours of changes to consumers' electronic banking passwords; (ii) were received within hours of changes in consumers' online account type or status; (iii) were received within hours of consumers first enrolling in online wire transfer services; (iv) would have, if accepted and Citibank executed wire transfers from consumers' accounts in the same amounts, resulted in a near-zero balances in consumers' bank accounts; (v) were received following intra-bank transfers from consumers' other bank accounts that left near-zero balances in those other bank accounts; (vi) were the first or one of the first ever sent by consumers after several years of account activity; and (vii) were received within hours of similar Payment Orders that had been cancelled or were unable to be verified; and

c. Citibank has not had sufficient controls and has not trained employees to

respond effectively in real-time to reject fraudulent Payment Orders in response to consumers' timely instructions to limit such activity. Specifically: (i) notices of fraudulent activity to Citibank's customer service representatives have not secured consumers' bank accounts such that scammers could no longer successfully execute fraudulent Payment Orders; (ii) long hold times on phone communications after consumers' notices of fraudulent activity have slowed consumers' efforts to secure accounts; (iii) notices of fraudulent activity via telephonic dial or email have not secured consumers' bank accounts such that scammers could no longer successfully execute fraudulent Payment Orders; and (iv) requirements to travel to local branches to secure accounts have left consumers' bank accounts vulnerable to scammers' fraudulent activity.

105. Citibank has not acted in good faith or in compliance with its customers instructions in connection with its handling of Payment Orders sent electronically via wire transfer requests in the following respects:

a. Citibank has accepted Payment Orders in the face of one or more of the red flags identified in the preceding paragraph, all of which are common indicators of potentially fraudulent activity that should trigger robust verification protocols;

b. Citibank has accepted Payment Orders after consumers had provided notice that those Payment Orders were unauthorized and the result of fraudulent activity; and

c. Citibank has substantially delayed contacting beneficiary banks to freeze or recall consumers' stolen funds after notice of fraudulent activity.

106. In addition, Citibank's standard-form denial letter, which appended no evidence, have described no findings, and have followed wholly inadequate investigations that often have not included basic interviews with affected consumers, have not satisfied Citibank's burden to

prove that it was more probable than not that it (i) acted in compliance with security procedures, (ii) acted in good faith, or (iii) adhered to consumers' instructions regarding Payment Orders.

107. As a consequence of Defendants' breaches of the U.C.C., Plaintiff is entitled to compensatory damages in an amount to be determined at trial, but in no event less than the amount of the fraudulent transfers, plus interest paid on a short-term loan that Plaintiff was forced into obtaining due to Citibank's failure to timely refund the money.

108. Defendants' breaches of the U.C.C. have caused, and continue to cause, Plaintiff economic damage and other direct and consequential damages and losses.

109. Punitive and exemplary damages are necessary in this case to deter Defendant Citibank and other national banks from wantonly and maliciously failing to implement commercially reasonable security measures and failure to refund fraudulent monies in a timely manner.

SECOND CAUSE OF ACTION

Conversion

Against Defendant Citibank

110. Plaintiff repeats and realleges each of the foregoing allegations as if fully and completely set forth herein.

111. Plaintiff was in lawful possession of $149,994.89 in its Citibank bank account. Plaintiff solely had the right to possess and control this money.

112. Defendant Citibank interfered with Plaintiff's money in a manner that infringed on Plaintiff's rights because Citibank processed three fraudulent wires that, had Citibank employed reasonable security measures, it would have caught prior to the wire transfers. Citibank's conduct directly caused Plaintiff to lose this money.

113. Lewis actually assumed control over a part of Plaintiff's money—specifically, $49,995.00, which was deposited into Lewis's bank account held and operated by Wells Fargo. Plaintiff solely had the right to control and possess this money, and thereby Citibank permitted Lewis to interfere with Plaintiff's property in a manner that infringed on Plaintiff's rights.

114. Mendez actually assumed control over a part of Plaintiff's money—specifically, $50,000.00, which was deposited into Mendez's bank account held and operated by TD Bank. Plaintiff solely had the right to control and possess this money, and thereby Citibank permitted Mendez to interfere with Plaintiff's property in a manner that infringed on Plaintiff's rights.

115. Fundora actually assumed control over a part of Plaintiff's money—specifically, $49,999.89, which was deposited into Fundora's bank account held and operated by Wells Fargo. Plaintiff solely had the right to control and possess this money, and thereby Citibank permitted Fundora to interfere with Plaintiff's property in a manner that infringed on Plaintiff's rights.

THIRD CAUSE OF ACTION

Fraud

Against Defendant Citibank

116. Plaintiff repeats and realleges each of the foregoing allegations as if fully and completely set forth herein.

117. Defendant Citibank made a material misrepresentation of fact when it advertised repeatedly to Plaintiff, and other consumers, that it employs reasonable security measures for its bank accounts.

118. Defendant Citibank knew of the falsity of this misrepresentation, because the company knew that more robust security measures were available and Defendant Citibank selected to utilize weak security measures that were unreasonable in light of commercial best practices.

119. Defendant Citibank made the false misrepresentation with the intent to induce Plaintiff, and other customers, to open bank accounts with Defendant Citibank.

120. Plaintiff justifiably relied on Citibank's misrepresentations, given Citibank's stature in the banking industry as one of the largest banks in the nation. Plaintiff further justifiably relied on Citibank's misrepresentations that the company employs reasonable security measures to stop fraudulent wire transfers.

121. Plaintiff suffered damages as a result of its reliance on Citibank's misrepresentations, and Plaintiff opened an account with Citibank, utilized the account for its business, and lost $149,994.89 due to Citibank's processing of three fraudulent wire transfers that, had Citibank employed reasonable security measures as it represented to Plaintiff, would not have occurred.

FOURTH CAUSE OF ACTION

Violation of New York General Business Law Section 349

Against Defendant Citibank

122. Plaintiff repeats and realleges each of the foregoing allegations as if fully and completely set forth herein.

123. The Defendants' actions were materially misleading, the actions were consumer-oriented and Hiteks was injured as a result

124. New York General Business Law Section 349 declares unlawful, *inter alia*, "[d]eceptive acts or practices in the conduct of any business, trade, or commerce or in the furnishing of any service in" New York.

125. By engaging in the deceptive acts and practices alleged herein, Defendant Citibank has engaged in deceptive and misleading practices in violation of New York General Business Law Section 349.

FIFTH CAUSE OF ACTION

Violation of New York General Business Law Section 350

Against Defendant Citibank

126. Plaintiff repeats and realleges each of the foregoing allegations as if fully and completely set forth herein.

127. New York General Business Law Section 350 prohibits "[f]alse advertising in the conduct of any business, trade or commerce or in the furnishing of any service in" New York.

128. New York General Business Law Section 350-a further provides that "false advertising" is advertising that is "misleading in a material respect."

129. By engaging in the advertising alleged above, Defendant Citibank has engaged in false advertising in violation of New York General Business Law Section 350.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Hiteks respectfully requests the following relief:

(1) Judgment against Defendant awarding compensatory, consequential, special, exemplary, and punitive damages in an amount to be determined at trial;

(2) Statutory damages and relief, as may be applicable;

(3) An award of plaintiff's attorneys' fees, costs, and disbursements accrued in pursuit of this action, and/or any other applicable statute; and

(4) Such other and further relief as the Court may deem just and proper.

JURY DEMAND

Plaintiff hereby demands a trial by jury on all causes of action asserted within this pleading.

Dated: New York, New York
October 30, 2024

SALZANO ETTINGER & LAMPERT LLP

By: _____
Jason Lampert, Esq.
Frank Salzano, Esq.
104 West 40th Street, 14th Floor
New York, New York 10018
Tel: (212) 375-6746

and

DEBENEDICTIS & DEBENEDICTIS LLC

By: _____
Michael J. DeBenedictis, Esq.
1415 Route 70 East. Suite 103
Cherry Hill, New Jersey 08034
Tel: (856) 795-2101

Attorneys for Plaintiff

citi

Wire Summary as of Nov 16, 2023 at 07:19 PM UTC

CitiBusiness® Online

WIRE TRANSFER DETAILS

Wire Transfer Status:**Complete**

Fed Ref/CHIPS: *20231108MMQFMPYZ005382* *Global ID:* *G0133122600301*

From

Account Name	---
Account Number	*****8065
Account Type	Checking
Set Up By	GERASIMOS PETRATOS

To

Beneficiary	Lourdes Thalice Leon Fundora
Beneficiary Account Number	[redacted]4868
ABA	1[redacted]0248
Beneficiary Address	630 SW 62nd Ave Miami, FL 33144
Beneficiary Phone	---
Bank Address	WELLS FARGO BANK, NA, CA
Special Instructions	NEED PAYMENT SENT EXPEDITIOUSLYFINALIZATION OF BUSINESS DEALRENOVATIONS COMPLETED

Scheduling & Dates

Date Submitted	11/08/2023
Date Completed	11/08/2023 06:01 AM

Amount & Additional Info

Amount	49,999.89 USD
Customer Reference No.	---
Citibank Reference No.	3120034969
Additional Reference	---

This information is provided for your convenience only. It is not a substitute for the periodic statement which is the official record of your account activity.

citi

Wire Summary as of Nov 16, 2023 at 07:21 PM UTC

CitiBusiness® Online

WIRE TRANSFER DETAILS

Wire Transfer Status:**Complete**

Fed Ref/CHIPS: *20231106MMQFMPYZ010614* *Global ID:* *G0133103481201*

From

Account Name	---
Account Number	*****8065
Account Type	Checking
Set Up By	GERASIMOS PETRATOS

To

Beneficiary	Ashani Lewis
Beneficiary Account Number	[redacted]6822
ABA	[redacted]0248
Beneficiary Address	111 Woodlawn Circle East Hartford, CT 06108
Beneficiary Phone	---
Bank Address	WELLS FARGO BANK, NA, CA
Special Instructions	NEED PAYMENT SENT URGENTBUSINESS DEAL CLOSING FOR RENOVATEAND REPAIRS

Scheduling & Dates

Date Submitted	11/06/2023
Date Completed	11/06/2023 10:08 AM

Amount & Additional Info

Amount	49,995.00 USD
Customer Reference No.	---
Citibank Reference No.	3100215917
Additional Reference	---

This information is provided for your convenience only. It is not a substitute for the periodic statement which is the official record of your account activity.

Wire Summary as of Nov 16, 2023 at 07:20 PM UTC

CitiBusiness® Online

WIRE TRANSFER DETAILS

Wire Transfer Status:**Complete**

Fed Ref/CHIPS: *20231107MMQFMPYZ005108* *Global ID:* *G0133112273601*

From

Account Name	---
Account Number	*****8065
Account Type	Checking
Set Up By	GERASIMOS PETRATOS

To

Beneficiary	Juliet Mendez
Beneficiary Account Number	[redacted]1703
ABA	[redacted]1266
Beneficiary Address	4744 N mascher st philedelphia, PA 19120
Beneficiary Phone	---
Bank Address	TD BANK, NA, DE
Special Instructions	NEED PAYMENT SENT EXPEDITIOUSLYBUSINESS DEAL CLOSING TO RENOVATE

Scheduling & Dates

Date Submitted	11/07/2023
Date Completed	11/07/2023 06:01 AM

Amount & Additional Info

Amount	50,000.00 USD
Customer Reference No.	---
Citibank Reference No.	3110262832
Additional Reference	---

This information is provided for your convenience only. It is not a substitute for the periodic statement which is the official record of your account activity.

AFFIDAVIT OF UNAUTHORIZED ONLINE WIRE TRANSFER

PLEASE PRINT LEGIBLY

citibank

Claimant Name (Business or Individual)	Account Number
HITEKS SOLUTIONS INC.	[redacted]8065
Street Address	**Home Telephone Number**
767 13TH AVENUE N	(917) 8421507
City, State, Zip, Country	**Business Telephone Number**
ST PETERSBURG FL 33701	( )

DESCRIBE DISPUTED ITEM

Date of Transaction	Drawer (i.e., maker)	Payable to the Order of	Amount
11/06/2023	HITEKS SOLUTIONS INC.	Lourdes Thalice Leon Fundora	$ 49,999.89

CLAIM DESCRIPTION

The item described above was improperly paid because of an:

☑ **Unauthorized Online Wire Transfer**
The online wire transfer was not authorized by me and I received no benefit from the issuance of this transfer. The person(s) who initiated this online wire transfer is not authorized to use this account(s).

CLAIMANT'S STATEMENTS

1. I did not receive any benefit or value from proceeds of the Online Wire Transfer, and proceeds were not used for any purpose on my behalf.
2. I have not arranged with the person(s) who initiated the Online Wire Transfer to be reimbursed for proceeds of the transaction. I do not carry any insurance applicable to the loss resulting from the transaction. I suspect:
   Juliet Mendez (Suspect Name) of, N/A (Suspect Address), of having initiated the unauthorized transaction described in this Affidavit, as I have stated above. I believe this person did this under the following circumstance:
   PERSONAL GAIN
3. I, the Claimant, was not negligent in contributing to the unauthorized Online Wire Transfer and discovered the transaction on
   11/08/2023 (date), under the following circumstances:
   ACCOUNT OVERVIEEW
4. I understand that Citibank is a federally insured bank and that making any false statements to Citibank in connection with my claims, or to induce Citibank to rely upon those statements, is a crime. I also understand that Citibank or other persons or entities, such as law enforcement may require my assistance in connection with any criminal or civil prosecution of the wrongdoer(s). Should that arise, I agree to cooperate fully, including the giving of testimony and appearing at a trial. Should I refuse to cooperate, Citibank may revoke any settlement it offered or paid to me, including charging the amount of any settlement to any account I hold at Citibank.
5. I declare under penalty of perjury under the laws of the State of NEWYORK (State) that the foregoing is true and correct.

Claimant's Signature	Date	If Claimant is a Business, Print Name/Title of Authorized Signer
X [signature]	11/10/2023	GERASIMOS PETRATOS, CEO

Notary Seal

State of NY

County of NY

Subscribed and sworn to (or affirmed) before me on this 10th day of NOV, 2023.

by Gerasimos Nicholas Petratos, personally known to me or proved to me on the basis of satisfactory evidence to be the person(s) who appeared before me.

JIANA HUANG
Notary Public - State of New York
NO. 01HU6204131
Qualified in Kings County
My Commission Expires Apr 13, 2025

[signature]
Notary Public Signature

© 2009 Citibank
Citibank, N.A. Member FDIC.

AFFIDAVIT OF UNAUTHORIZED ONLINE WIRE TRANSFER

PLEASE PRINT LEGIBLY

citibank

Claimant Name (Business or Individual)	Account Number
HITEKS SOLUTIONS INC.	[redacted]8065
Street Address	**Home Telephone Number**
767 13TH AVENUE N	(917) 8421507
City, State, Zip, Country	**Business Telephone Number**
ST PETERSBURG FL 33701	( )

DESCRIBE DISPUTED ITEM

Date of Transaction	Drawer (i.e., maker)	Payable to the Order of	Amount
11/06/2023	HITEKS SOLUTIONS INC.	Juliet Mendez	$ 50,000.00

CLAIM DESCRIPTION

The item described above was improperly paid because of an:

☑ **Unauthorized Online Wire Transfer**
The online wire transfer was not authorized by me and I received no benefit from the issuance of this transfer. The person(s) who initiated this online wire transfer is not authorized to use this account(s).

CLAIMANT'S STATEMENTS

1. I did not receive any benefit or value from proceeds of the Online Wire Transfer, and proceeds were not used for any purpose on my behalf.
2. I have not arranged with the person(s) who initiated the Online Wire Transfer to be reimbursed for proceeds of the transaction. I do not carry any insurance applicable to the loss resulting from the transaction. I suspect:
   Juliet Mendez (Suspect Name) of, N/A (Suspect Address), of having initiated the unauthorized transaction described in this Affidavit, as I have stated above. I believe this person did this under the following circumstance:
   PERSONAL GAIN
3. I, the Claimant, was not negligent in contributing to the unauthorized Online Wire Transfer and discovered the transaction on
   11/08/2023 (date), under the following circumstances:
   ACCOUNT OVERVIEEW
4. I understand that Citibank is a federally insured bank and that making any false statements to Citibank in connection with my claims, or to induce Citibank to rely upon those statements, is a crime. I also understand that Citibank or other persons or entities, such as law enforcement may require my assistance in connection with any criminal or civil prosecution of the wrongdoer(s). Should that arise, I agree to cooperate fully, including the giving of testimony and appearing at a trial. Should I refuse to cooperate, Citibank may revoke any settlement it offered or paid to me, including charging the amount of any settlement to any account I hold at Citibank.
5. I declare under penalty of perjury under the laws of the State of NEWYORK (State) that the foregoing is true and correct.

Claimant's Signature	Date	If Claimant is a Business, Print Name/Title of Authorized Signer
X [signature]	11/10/2023	GERASIMOS PETRATOS, CEO

Notary Seal

State of NY

County of NY

Subscribed and sworn to (or affirmed) before me on this 10th day of NOV, 2023,
by Gerasimos Nicholas Petratos, personally known to
me or proved to me on the basis of satisfactory evidence to be the person(s) who appeared before me.

JIANA HUANG
Notary Public - State of New York
NO. 01HU6204131
Qualified in Kings County
My Commission Expires Apr 13, 2025

[signature]
Notary Public's Signature

© 2009 Citibank
Citibank, N.A. Member FDIC.

AFFIDAVIT OF UNAUTHORIZED ONLINE WIRE TRANSFER

citibank

PLEASE PRINT LEGIBLY

Claimant Name (Business or Individual)	Account Number
HITEKS SOLUTIONS INC.	[redacted]3065
Street Address	**Home Telephone Number**
767 13TH AVENUE N	(917) 8421507
City, State, Zip, Country	**Business Telephone Number**
ST PETERSBURG FL 33701	( )

DESCRIBE DISPUTED ITEM

Date of Transaction	Drawer (i.e., maker)	Payable to the Order of	Amount
11/06/2023	HITEKS SOLUTIONS INC.	Ashani Lewis	$ 49,995.00

CLAIM DESCRIPTION

The item described above was improperly paid because of an:

☑ **Unauthorized Online Wire Transfer**
The online wire transfer was not authorized by me and I received no benefit from the issuance of this transfer. The person(s) who initiated this online wire transfer is not authorized to use this account(s).

CLAIMANT'S STATEMENTS

1. I did not receive any benefit or value from proceeds of the Online Wire Transfer, and proceeds were not used for any purpose on my behalf.
2. I have not arranged with the person(s) who initiated the Online Wire Transfer to be reimbursed for proceeds of the transaction. I do not carry any insurance applicable to the loss resulting from the transaction. I suspect:
   Ashani Lewis (Suspect Name) of, N/A (Suspect Address), of having initiated the unauthorized transaction described in this Affidavit, as I have stated above. I believe this person did this under the following circumstance:
   PERSONAL GAIN
3. I, the Claimant, was not negligent in contributing to the unauthorized Online Wire Transfer and discovered the transaction on
   11/08/2023 (date), under the following circumstances:
   ACCOUNT OVERVIEEW
4. I understand that Citibank is a federally insured bank and that making any false statements to Citibank in connection with my claims, or to induce Citibank to rely upon those statements, is a crime. I also understand that Citibank or other persons or entities, such as law enforcement may require my assistance in connection with any criminal or civil prosecution of the wrongdoer(s). Should that arise, I agree to cooperate fully, including the giving of testimony and appearing at a trial. Should I refuse to cooperate, Citibank may revoke any settlement it offered or paid to me, including charging the amount of any settlement to any account I hold at Citibank.
5. I declare under penalty of perjury under the laws of the State of NEWYORK (State) that the foregoing is true and correct.

Claimant's Signature	Date	If Claimant is a Business, Print Name/Title of Authorized Signer
X [signature]	11/10/2023	GERASIMOS PETRATOS, CEO

Notary Seal

State of NY
County of NY

Subscribed and sworn to (or affirmed) before me on this 10th day of Nov., 2023
by Gerasimos Nicholas Petratos, personally known to me or proved to me on the basis of satisfactory evidence to be the person(s) who appeared before me.

JIANA HUANG
Notary Public - State of New York
NO. 01HU6204131
Qualified in Kings County
My Commission Expires Apr 13, 2025

[signature]
Notary Public Signature

© 2009 Citibank
Citibank, N.A. Member FDIC.

New York City Police Department

Omniform System - Complaints

Report Cmd:	Jurisdiction:	ICAD#:	Record Status:	Public Omni	Complaint #:	No Other Legacy Blue Versions	Complaint Revisions:
001	N.Y. POLICE DEPT		Final, No Arrests	NO	2023-001-009850		View All Versions 0 1

Occurrence INSIDE OF 447
Location: BROADWAY
Name Of Premise:
Premises Type: COMMERCIAL BUILDING
Location Within Premise:
Visible By Patrol?: NO

NYC Parks Dept. Property
Did this offense occur on NYC Parks Dept. Property? NO
Command:
NYC Parks Dept. Property Name:

Precinct: 001
Sector: D
Beat:
Post:

Occurrence From: 2023-11-06 10:08 MONDAY
Occurrence thru: 2023-11-08 06:01
Reported: 2023-12-09 10:22
Complaint Received: WALK-IN

Aided #
Accident #
O.C.C.B. #

Classification: IDENTITY THEFT, UNLA
Attempted/Completed: COMPLETED
Most Serious Offense Is: FELONY
PD Code: 739 FRAUD, UNCLASSIFIED-FELONY
PL Section: 19080
Keycode: 112 THEFT-FRAUD

Case Status: OPEN
Unit Referred To: P.D.U.
Clearance Code:
Log/Case #: 0
Clearance Arrest Id:
Clearance AO Cmd:
File #:
Prints Requested? NO

OFFENSES:

Order	Offense Desc	Att/Cmplt	PDC Code	PDC Code Desc	PL Section	PL Description	Larceny Type	IBR#	Class	Alleged Crime	Justified Crime	Criminal Activity
1	PL 190 ISSUING A BAD CHECK	COMPLETED	739	FRAUD, UNCLASSIFIED-FELONY	PL 190.80 03	IDENTITY THEFT 1-COMMIT FELONY		26F	Felony			

Confirmed Shots Fired? NO

Possible Hate Crime ? NO

Is This Related To Stop And Frisk Report	SQF Number:	Was The Victim's Personal Information Taken Or Possessed?	Was The Victim's Personal Information Used To Commit A Crime?
NO	0000-000-00000	NO	NO

Gang Related?	Detective Borough Wheel Log #:	Name Of Gang:	Child Abuse Suspected?
NO			NO

DIR Required?	Child in Common?	Intimate Relationship?	Officer Body Worn Camera:
NO	NO	NO	NO

If Burglary:
Forced Entry?
Structure:
Entry Method:
Entry Location:

Alarm:
Bypassed?
Comp Responded?:
Company Name/Phone:
- -
Crime Prevention Survey Requested?:
Complaint/Reporter Present?:

If Arson:
Structure:
Occupied?:
Damage by:

Taxi Robbery:
Partition Present:
Amber Stress Light Activated:
Method of Conveyance:
Location of Pickup:

Supervisor On Scene - Rank / Name / Command :	Canvas Conducted:	Translator(if used):
	NO	

NARRATIVE:
AT T/P/O, R/W STATES, ON THREE SEPARATE DATES (11/6/2023, 11/7/2023, 11/8/2023), A TOTAL OF 149,994.89 USC WAS WIRED FROM HIS CITI BANK BUSINESS ACCOUNT WITHOUT PERMISSION OR AUTHORITY.

Version 1. OVER THE COURSE OF 11/06/2023 TO 11/08/2023 USC WAS SENT TO 3 DIFFERENT LOCAT ONS. $49,995 WAS SENT TO A WELLS FARGO

IN HARTFORD CT. $50,000 WAS SENT TO A D BANK IN PHILADELPHIA PA. $49,999 WAS SENT TO A WELLS FARGO IN MIAMI FL. ALL TRANSACTIONS WERE OUTSIDE THE CONFINES OF NYC

No NYC TRANSIT Data for Complaint # 2023-001-009850

Total Victims:	Total Witnesses:	Total Reporters:	Total Wanted:
1	0	1	1

VICTIM: # 1 of 1

Name: HITEKS REAL-TIME SOLUTIONS
Complaint#: 2023-001-009850

Nick/AKA/Maiden:
UMOS:
Sex/Type: / BUSINESS
Race: UNKNOWN
Age: 0
Date Of Birth: UNKNOWN
Disabled? NO
Is this person not Proficient in English?:
If Yes, Indicate Language:
N.Y.C.H.A Resident?
Is Victim fearful for their safety / life?
Escalating violence / abuse by suspect?
Were prior DIR's prepared for C/V?

Suspected Gang Member: NO
Name:

Will View Photo: YES
Will Prosecute: YES
Notified Of Crime Victim Comp. Law: YES

LOCATION	ADDRESS	CITY	STATE/COUNTRY	ZIP	APT/ROOM
BUSINESS	447 BROADWAY	MANHATTAN	NEW YORK		2FL

Phone #: HOME: Not Provided/Unavailable CELL: Not Provided/Unavailable BUSINESS:212-920-0929 BEEPER: Not Provided/Unavailable E-MAIL: Not Provided/Unavailable

Action against Victim:

Actions Of Victim Prior To Incident:
VICTIM WAS OPERATING DURING BUSINESS HOURS

Victim Of Similar Incident:
NO

If Yes, When And Where

REPORTER: # 1 of 1

Name: PETRATOS,GERASIMOS
Complaint #: 2023-001-009850

Nick/AKA/Maiden:
Sex/Type: MALE
Race: WHITE
Age: 049
Date Of Birth: [redacted]
Is this person not Proficient in English?: NO
If Yes, Indicate Language:

Suspected Gang Member: NO
Name:

Relationship To Victim: EMPLOYER

Location	Address	City	State/Country	Zip	Apt/Room
HOME-PERMANENT	767 13 AVENUE N	ST PETERSBURG	FLORIDA	33701	

Phone #: HOME: - - CELL: 917-842-1507 BUSINESS:212-920-0929 BEEPER: - - E-MAIL: GERRY@HITEKS.COM

WANTED: # 1 of 1

Name: UNKNOWN ONE, UNKNOWN ONE
Complaint#: 2023-001-009850
Arrested: NO

Nick/AKA/Maiden:
Sex: UNKNOWN
Race:
Age:
Date Of Birth: UNKNOWN
U.S. Citizen:
Place Of Birth:
Is this person not Proficient in English?:
If Yes, Indicate Language:
Accent: NO

Height: FTIN
Weight: 0
Eye Color: UNKN
Hair Color: UNKNWN
Hair Length:
Hair Style: UNKNOWN
Skin Tone: UNKN
Complexion: UNKNOWN
Offender Condition: UNKNOWN
S.S. #: 0

Order Of Protection: NO
Issuing Court:
Docket #:
Expiration Date:
Order of Protection Violated?
Does Suspect abuse Drugs / Alcohol? NO
Suspect threatened /attempted suicide? NO
Is the suspect Parole / Probation? NO
Relation to Victim: NO RELATIONSHIP
Living together: NO
Can be Identified: NO

Suspected Gang Member: NO
Name:

LOCATION	ADDRESS	CITY	STATE/COUNTRY	ZIP	APT/ROOM	HOW LONG?	RES. PCT
HOME-PERMANENT							

Phone #: HOME: - - CELL: - - BUSINESS: - - BEEPER: - - E-MAIL:

N.Y.C.H.A. Resident: N.Y.C. Housing Employee: On Duty:
Development: N.Y.C. Transit Employee:

Weapons:

1 Physical Force/Weapon: NONE Firearm Recovered: Serial Number Defaced:
Physical Force/Weapon Type: Discharged: NO Serial Number:
Physical Force/Weapon Sub Type: Make:
Specific Physical Force/Weapon Type: Color:
Other Weapon Description: Caliber:

Used Transit System:
Station Entered:
Time Entered:
Metro Card Type:
Metro Card Used/Poses:
Card #:

CRIME DATA	DETAILS
STATEMENTS MADE	UNK
METHOD OF FLIGHT	UNK
MODUS OPERANDI	UNKNOWN
ACTIONS TOWARD VICTIM	UNK
CLOTHING	ACCESSORIES -UNK -UNKNOWN COLOR
CLOTHING	FOOTWEAR -UNK -UNKNOWN COLOR
CLOTHING	HEADGEAR -UNK -UNKNOWN COLOR
CLOTHING	OUTERWEAR -UNK -UNKNOWN COLOR
CHARACTERISTICS	UNKNOWN
BODY MARKS	-UNKNOWN
IMPERSONATION	UNKNOWN

PROPERTY:

Complaint #2023-001-009850

Lost/Stolen/Found: STOLEN

Item	Property Involvement	Property Category	Type	Recovered	Owner Identification Num:	Qty	Description	Serial #	$ Value	$ Recovered
1.	STOLEN	CURRENCY	MONEY	NO	NONE	1.	149,994.84 USC		149994.	0.

TOTAL VALUES: STOLEN $ 149994. RECOVERED $ 0.

EVIDENCE:

Complaint # 2023-001-009850

Evidence Collected?:	Evidence Collection Team/Crime Scene Requested?:	ECT Responded?:	ECT Run#:	Crime Scene Responded?:	Crime Scene Number:
NO	NO	NO		NO	-

Evidence Invoice #

No IMEI Data for Complaint # 2023-001-009850

SCRATCH COPY:

Complaint # 2023-001-009850

1	 1702145161594_1702145161594_.pdf	Description 1702145161594_1702145161594_.pdf

COMPLAINT ASSOCIATIONS: | **Complaint # 2023-001-009850**

Victim	Perpetrator/Wanted	Relationship	Interaction	Offense	Weapon/Force	Weapon/Force Type	Weapon/Force Sub Type	Specific Weapon/Force Type	Description
HITEKS REAL-TIME SOLUTIONS	UNKNOWN ONE, UNKNOWN ONE	NO RELATIONSHIP	Yes	PL 190					

NOTIFICATIONS / ADDITIONAL COPIES: | **Complaint # 2023-001-009850**

Notifications to:

Rank/Title	Name	Unit/Agency	Log #
CO	ROSENTHAL	1 CO	
SGT	RIVERA	1 DESK	
DET	GERMAN	1 PDU	

Reporting/Investigating M.O.S. Name: PO PANTON DAJON	**Tax #:** 959872	**Command:** 001 PCT	**Rep.Agency:** NYPD
Supervisor Approving Name: SGT RIVERA ADRIANO	**Tax #:** 949906	**Command:** 001 PCT	**Rep.Agency:** NYPD
Complaint Report Entered By: PO PANTON	**Tax #:** 959872	**Command:** 001 PCT	**Rep.Agency:** NYPD
Signoff Supervisor Name: SGT RIVERA	**Tax #:** 949906	**Command:** 001 PCT	**Rep.Agency:** NYPD

END OF COMPLAINT REPORT
 # 2023-001-009850

CITIBANK N.A.
Fraud Prevention
P.O. Box 769027-9027
San Antonio, TX 78245-9963

Decision on Fraud Claim **Claim Number 00132952935**

02/10/2024

HITEKS SOLUTIONS INC
Attn: GERASIMOS PETERATOS
447 BROADWAY FLOOR 2
NEW YORK NY 10013

www.citibank.com

Re: Unauthorized Wire Claim on Account ending in 8065 for transaction(s) posted between November 06, 2023 and November 08, 2024, for a total amount of $149,994.89

Dear GERASIMOS PETERATOS,

Why We're Writing to You

We have completed our investigation of your fraud claim. Please note that it has been denied. Our decision was based on:

What You Need to Know

- The above-referenced transaction(s) were verified using an authentication process with your device(s) and/or confidential information. Pursuant to Citibank's security procedures, the payment order was therefore accepted as your authenticated request. As such, we are unable to honor your claim.

How To Contact Us

If you have any questions, our Centralized Disputes Unit representatives may be contacted toll-free Monday – Friday, 7:00 a.m. to 11:00 p.m. ET, Saturday, 9:00 a.m. to 7:30 p.m. ET, and Sunday, 9:00 a.m. to 5:30 p.m. at:

- Toll Free 1-833-782-1456 Letter Code: 7150
- International Calls 1-210-677-0065
- For TTY: We accept 711 or other Relay Service
- The number on the back of your Citibank Banking Card

We appreciate your business with Citibank and look forward to serving all your future financial needs.

Sincerely,

Citibank Fraud Prevention

Calls are randomly monitored and recorded to ensure quality service.
Please consult the Citibank Client Manual- Consumer Accounts for important conditions and limitations.
Fraud Control & Risk Management performs risk management functions for Citibank, N.A.
©2024 Citibank, N.A. Member FDIC. Citi, Citi and Arc Design and other marks used herein are service marks of Citigroup Inc. or its affiliates, used and registered throughout the world. All rights reserved.

"Examining Scams and Fraud in the Banking System and Their Impact on Consumers"

U.S. Senate Committee on Banking, Housing, and Urban Affairs

Thursday, February 1, 2024

Testimony of Carla Sanchez-Adams

National Consumer Law Center
on behalf of its low-income clients

National Consumer Law Center

"Examining Scams and Fraud in the Banking System and Their Impact on Consumers"

U.S. Senate Committee on Banking, Housing, and Urban Affairs

Testimony of Carla Sanchez-Adams

Thursday, February 1, 2024

Chairman Brown, Ranking Member Scott, and Members of the Committee, thank you for inviting me to testify today regarding scams and fraud in the banking system and their impact on consumers. I am Carla Sanchez-Adams, a senior attorney at the National Consumer Law Center. I offer my testimony on behalf of NCLC's low-income clients.

Since 1969, the nonprofit National Consumer Law Center® (NCLC®) has used its expertise in consumer law and energy policy to work for consumer justice and economic security for low-income and other disadvantaged people in the United States. NCLC's expertise includes policy analysis and advocacy; consumer law and energy publications; litigation; expert witness services; and training and advice for advocates. NCLC works with nonprofit and legal services organizations, private attorneys, policymakers, and federal and state government and courts across the nation to stop exploitative practices, help financially stressed families build and retain wealth, and advance economic fairness. NCLC has long advocated for stronger laws, regulation, and enforcement to ensure that consumers' funds and payments are safe and to prevent and remedy fraud.

I am one of the co-authors of NCLC's treatise, Consumer Banking and Payments Law. My colleagues and I interact with legal services, government, and private attorneys, as well as community groups and organizations from all over the country who represent low-income and vulnerable individuals on consumer issues. As a result of our daily contact with these advocates, we have seen many examples of the damage wrought by payment fraud from every part of the nation. It is from this vantage point that I supply this testimony.

NCLC has previously provided testimony before Congress on the need to address payment fraud.[1] Additionally, NCLC has provided feedback to various regulatory agencies on the same issue.[2] I reiterate and incorporate those comments here as well.

Payment fraud impacts all Americans across many communities— young, old, those highly educated, and those that are not. But the impacts of fraud are most keenly felt by certain vulnerable populations such as older Americans, low-income consumers, and minorities.

Consumers are plagued by problems with unauthorized transactions as well as fraudulently induced transactions over peer-to-peer payment applications, bank-to-bank wire transfers, check alterations and forgeries, and Electronic Benefits Transfer card skimming, The increasing ease

[1] *See* NCLC *et al*., Statement for the Record, "*What's in Your Digital Wallet? A Review of Recent Trends in Mobile Banking and Payments*," Hearing Before the House Financial Services Taskforce on Financial Technology at 10-11 (April 28, 2022), available at https://www.govinfo.gov/content/pkg/CHRG-117hhrg47649/pdf/CHRG-117hhrg47649.pdf; Testimony of Odette Williamson, NCLC *"Fraud, Scams and COVID-19: How Con Artists Have Targeted Older Americans During the Pandemic,"* Hearing Before the U.S. Senate Special Committee on Aging (Sept. 23, 2021) available at https://www.nclc.org/wp-content/uploads/2022/08/Testimony_Covid_Aging-1.pdf.

[2] *See* NCLC *et al*., Comments regarding the FTC Collaboration Act of 2021, (Aug. 14, 2023) available at https://www.nclc.org/wp-content/uploads/2023/08/FTC_AG-Fraud-Collaboration-consumer-comments-8-14-23-final3-Lauren-Saunders.pdf; NCLC *et al.,* Letter Urging Federal Reserve Board to Prevent FedNow Errors and Fraud, (Aug. 10, 2022) available at https://www.nclc.org/wp-content/uploads/2022/09/FedNow_fraud_ltr.pdf; Comments of 43 consumer, small business, civil rights, community and legal service groups to Federal Reserve Board Re: Collection of Checks and Other Items by Federal Reserve Banks and Funds Transfers Through Fedwire, Docket No. R-1750; RIN 7100-AG16 (Sept. 9, 2021), https://bit.ly/FedNowCoalitionComments ("FedNow Comments").

and use of mobile and online banking through technological advancement have also simultaneously provided opportunities for scammers to exploit newer payment technologies. However, obtaining a complete and holistic picture of the volume, loss, and threat of payment fraud is difficult because of the fragmented way we collect this data.

The financial institutions that design and run these payment systems, including the financial institutions that hold the accounts of scammers and money mules that receive fraudulent payments, need to take more responsibility for making these systems safe and protecting consumers. Given the increasing sophistication of fraud schemes, warnings to consumers are insufficient. If payment system participants take responsibility for protecting consumers, as they are doing in the United Kingdom, they will have the incentive to leverage the latest innovative technologies to prevent and detect fraud, making the entire system safe. At the same time, any attempts to combat fraud must also be tempered with policies and procedures that protect innocent consumers who do not engage in payment fraud but whose funds might be frozen for extended periods of time.

To combat payment fraud, we recommend addressing the current gaps and ambiguities in the Electronic Funds Transfer Act that leave consumers unprotected. These include:

- Ensuring consumers are protected from liability when they are defrauded into initiating a transfer;
- Allowing the consumer's financial institution, after crediting the consumer for a fraudulent transfer, to be reimbursed by the financial institution that allowed the scammer to receive the fraudulent payment;
- Eliminating the exemption for bank wire transfers and electronic transfers authorized by telephone call, bringing those transfers within the EFTA and its protections against unauthorized transfers and errors;
- Eliminating the exclusion of Electronic Benefit Transfer cards from the EFTA, bringing those transfers within the EFTA and its protections against unauthorized transfers and errors;
- Clarifying that the EFTA's error resolution procedures apply when the consumer makes a mistake, such as in amount or recipient;
- Clarifying that the error resolution duties under the EFTA apply if a consumer's account is frozen or closed or the consumer is otherwise unable to access their funds, with an exception if the consumer was denied access due to a court order or law enforcement or the consumer obtained the funds through unlawful or fraudulent means; and
- Considering whether consumer protections for checks should be included in the EFTA.

Federal regulators should also take additional steps to address fraud and protect innocent consumers who are harmed by aggressive fraud reporting. For example, federal regulators should:

- Devote more attention to the responsibilities of institutions that receive fraudulent payments, including stepping up enforcement of Bank Secrecy Act /Anti-Money Laundering obligations;

- Establish interagency collaboration to assist consumers with reporting fraud, collecting data on fraud, and establishing systems; and
- Provide guidance to financial institutions about the timelines and procedures for consumers to regain access to improperly frozen funds and clarify what information can and should be given to accountholders regarding account closures and freezes.

I. Fraud is Exploding and Affects Everyone.

Fraud continues to climb and devastates millions of consumers across the country each year. In 2022, the Federal Trade Commission (FTC) received over 2.5 million reports of fraud with reported losses totaling almost $9 billion ($8,996,000). Those losses are up a shocking 46.7% over 2021. Losses for 2023, which have not yet been fully reported, are on track to exceed 2022.

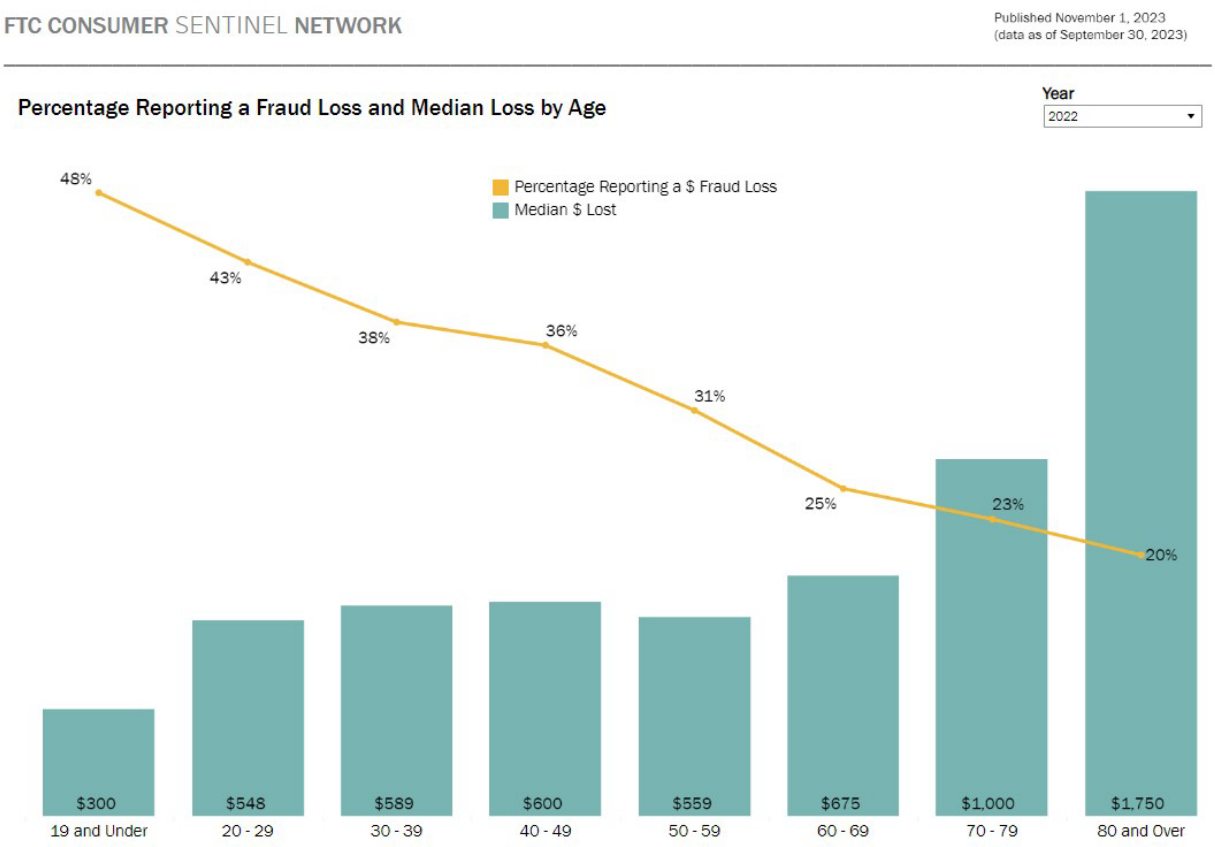
Additionally, the FTC numbers reflect only fraud cases reported to the FTC. Fraud is substantially underreported; only an estimated 15% of U.S. fraud victims report the fraud to law enforcement.[3]

As AARP noted:

> "While nearly nine in 10 respondents (87%) feel people should report incidents of fraud, only an estimated 15% contact law enforcement. The gap may be tied to attitudes and awareness about fraud. Sometimes those who have been victimized by a scam feel embarrassed, guilty, or believe there is nothing police can do."[4]

Fraud impacts all of us, across every community— the young and the old, those highly educated and those that are not.[5] While the common belief is that older consumers are more likely to be susceptible, in fact younger people are significantly more likely to experience fraud. But when older people suffer fraud, they lose far more money, as shown by the following FTC chart:[6]

[3] Department of Justice, U.S. District Attorney's Office, District of Alaska, Financial Crime Fraud Victims (2020), https://www.justice.gov/usao-ak/financial-fraud-crimes.
[4] Williams, Alicia R., "*Americans Are Aware of Fraud's Pervasiveness but Remain Vulnerable*," AARP Research (May 17, 2023); *see* Department of Justice, U.S. District Attorney's Office, District of Alaska, Financial Crime Fraud Victims (2020), https://www.justice.gov/usao-ak/financial-fraud-crimes.
[5] Levinthal, Dave, "*Cyberthieves stole $186,000 from a Republican member of Congress as fraud epidemic plagues political committees*," Business Insider (Nov. 29, 2022) available at https://www.businessinsider.com/online-fraud-congress-diana-harshbarger-cybertheft-2022-11.
[6] FTC, Percentage Reporting a Fraud Loss and Median Loss by Age (2022), *available at* https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/FraudLosses.



Fraud has a particularly harsh impact on low-income families and communities of color, who have fewer resources to help them recover. Fraudsters often take the last dollar from those least able to afford it, and often target older adults, immigrants, and other communities of color.

II. Payment Systems Play an Important Role in Enabling or Preventing Fraud and in Protecting Consumers.

Criminals who steal money through fraud schemes need a way to obtain a victim's money. They use a variety of payment systems to receive that money, including person-to-person (P2P) transfer services, wire transfers, checks, and gift cards. Each of those payment systems has a role to play in keeping criminals out, preventing fraud, and protecting consumers. Fraud does not succeed if the fraudster cannot receive the money.

Fraud may result in unauthorized transactions or fraudulently induced transactions, each with different protections. After obtaining information through phishing schemes, fraud schemes, or data breaches, criminals may make unauthorized transactions for which consumers generally have protection (though, in some cases, imperfect protection, as discussed below). Checks can also be stolen and altered, another form of unauthorized transaction. Or criminals can defraud a consumer into making a fraudulently induced transaction where protection is sorely lacking.

As discussed in more detail below, payment fraud usually involves two institutions – the institution that holds the consumer's account (the consumer's institution) and the institution that

receives the stolen funds and holds the account of the fraudster or money mule (the receiving institution). When seeking to prevent and remedy fraud, it is important to focus on the responsibilities of both the consumer's institution and the receiving institution as well as the payment system itself, regardless of whether the fraud is unauthorized or fraudulently induced. When consumers are protected, these institutions and systems will have incentives to use their resources and technological innovations to prevent fraud and make everyone safer.

In the testimony below I will focus on four payment vehicles that have seen increasing fraud: person-to-person payments, bank-to-bank wire transfers, check alterations, and Electronic Benefit Transfer cards. I will discuss how these payment frauds impact consumers and how protections can be improved. I will also discuss the need for more data sharing in the effort to combat fraud.

III. Person-to-Person (P2P) Payment Fraud.

A. The prevalence of P2P use and the incidence of fraud on these platforms.

Person-to-person (P2P) payment apps have become increasingly popular among consumers. Seventy-six percent of households use Venmo or Cash App.[7] In addition to P2P payment services, consumers are also increasingly adopting other forms of technology to make payments.[8]

According to the FTC,[9] "payment app or service" is the third largest category of payment method specified by fraud victims in terms of number of reports (after credit cards and debit cards), and the dollar volume of losses by payment app or service increased 25% from 2021 to 2022.[10] Though the final figures of fraud reports are unavailable for 2023, the FTC received reports during the first three quarters of 2023 that are on path for another 25% increase by dollar amount of losses.[11] The Consumer Financial Protection Bureau (CFPB) has also seen high growth in complaints about fraud in P2P apps and digital wallets.[12]

As consumer, small business, civil rights, community, and legal service groups described at greater length in comments submitted to the Federal Reserve Board (FRB) and the CFPB, the existing P2P payment systems of large technology companies and financial institutions simply

---

[7] Anderson, Monica, "*Payment Apps like Venmo and Cash App Bring Convenience – and Security Concerns – to Some Users*," Pew Research Center (blog), (Sept. 8, 2022), available at https://www.pewresearch.org/short-reads/2022/09/08/payment-apps-like-venmo-and-cash-app-bring-convenience-and-security-concerns-to-some-users/.
[8] Chen, Jane, Deepa Mahajan, Marie-Claude Nadeau, and Roshan Varadarajan, "*Consumer Digital Payments: Already Mainstream, Increasingly Embedded, Still Evolving*," Digital Payments Consumer Survey, (Oct. 20, 2023), available at https://www.mckinsey.com/industries/financial-services/our-insights/banking-matters/consumer-digital-payments-already-mainstream-increasingly-embedded-still-evolving.
[9] Reports of fraud to the FTC do not always specify the payment method utilized to perpetuate the fraud; however, the FTC does collect and report data on payment method when available.
[10] FTC fraud reports by payment method available at https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/PaymentContactMethods. Only 429,264 (17%) of 2,563,959 fraud reports received by the FTC specified the payment method.
[11] *Id.*
[12] U.S. PIRG Educ. Fund, *Virtual Wallets, Real Complaints,* at 2, (June 2021), available at https://uspirg.org/sites/pirg/files/reports/VirtualWallets/Virtualwallets_USP_V3.pdf.

are not safe for consumers to use.[13]

P2P fraud has a particularly harsh impact on low-income families and communities of color. These communities, already struggling and often pushed out of the traditional banking system, can least afford to lose money to scams and errors. Because many minorities are also unbanked or underbanked,[14] they are the target audience for use of many of the P2P apps. For example, a September 2022 Pew Research Center survey shows that 59% of Cash App users are Black and 37% are Hispanic.[15] Yet Cash App has also been subject to reports of widespread fraud,[16] failing to protect the very vulnerable populations it targets.

The news media has reported many of the fraudulent schemes enabled by the P2P systems. Generally, these scams and theft would not have been possible without the payment apps.

- Manhattan District Attorney Alvin Bragg explains how criminals have utilized deception, violence, or threat of violence to steal funds from consumers through payment apps like Cash App.[17]

- Mary Jones of Kansas City paid $1,700 through Venmo in "rent" to a man who claimed to own the house she wanted to move into. He even gave them access to tour the house before she signed the lease. After she saw a "For Lease" sign in the front yard, she called the rental company and discovered that she had paid a scammer. She filed a police report but has not been able to retrieve her money.[18]

- In a similar fraud scheme, a single mom in South Carolina looking for housing paid a deposit, cleaning fee, and first month's rent on a condo listed on Redfin.com through a payment app and lost $2,600.[19]

---

[13] *See* Comments of 65 Consumer, Civil Rights, Faith, Legal Services and Community Groups to CFPB on Big Tech Payment Platforms at 4-5, Docket No. CFPB-2021-0017 (Dec. 21, 2021), https://bit.ly/CFPB-BTPS-comment ("CFPB Big Tech Payment Platform Comments"); Comments of 43 consumer, small business, civil rights, community and legal service groups to Federal Reserve Board Re: Collection of Checks and Other Items by Federal Reserve Banks and Funds Transfers Through Fedwire, Docket No. R-1750; RIN 7100-AG16 (Sept. 9, 2021), https://bit.ly/FedNowCoalitionComments (FedNow Comments).

[14] 11.3 percent of Black and 9.3 percent of Latino households are unbanked compared to only 2.1% of white households. *See* FDIC, *2021 FDIC National Survey of Unbanked and Underbanked Households*, at 2, https://www.fdic.gov/analysis/household-survey/2021report.pdf (last updated July 24, 2023).

[15] Anderson, Monica, "*Payment apps like Venmo and Cash App bring convenience – and security concerns – to some users,*" Pew Research Center (Sept. 8, 2022) available at https://www.pewresearch.org/short-reads/2022/09/08/payment-apps-like-venmo-and-cash-app-bring-convenience-and-security-concerns-to-some-users/.

[16] Hindenburg Research, "*Block: How Inflated User Metrics and 'Frictionless' Fraud Facilitation Enabled Insiders To Cash Out Over $1 Billion*," (Mar. 23, 2023), available at https://hindenburgresearch.com/block/. ("Former employees estimated that 40%-75% of accounts they reviewed were fake, involved in fraud, or were additional accounts tied to a single individual").

[17] Morales, Mark, "*Venmo and other payment app theft is 'skyrocketing,' Manhattan DA warns*," CNN (Jan. 23, 2024), available at https://www.cnn.com/2024/01/23/business/venmo-payment-app-theft?cid=ios_app.

[18] Johnson, Tia, "*Kansas City woman warns others after losing nearly $2,000 in rental home scam*," Fox4 (May 3, 2021), available at https://fox4kc.com/news/kansas-city-woman-warns-others-after-losing-nearly-2000-in-rental-home-scam/.

[19] Cioppa, Jordan, "*James Island woman says rental scam cost her $2,600*," WCBD News2 (Jan. 10, 2023), available at https://www.counton2.com/news/james-island-woman-says-rental-scam-cost-her-2600/.

Zelle is another popular P2P payment service, but users transfer funds between bank accounts directly.[20] As more and more consumers use Zelle, the service has also become popular among criminals.[21] For example:

- Maria Glover from Philadelphia had thousands of dollars stolen from her Citibank account via Zelle. She was contacted by the fraudsters through texts though she never provided any password or personal information to them. She further explains that the transactions stolen were for more than her $2,500 daily withdrawal limit, and Citibank could not even explain how the fraud occurred.[22]

- Luke Krafka, a professional musician in Long Island, lost almost $1,000 dollars through Zelle when a fake client "hired" him to play at a wedding. The man sent him a large check and asked him to pay part of the money back through Zelle. The check bounced after Krafka had already sent the money. His bank refused to refund his payment.[23]

P2P payment systems, if properly designed, can provide broad benefits to consumers. But those benefits will only be realized if the systems are safe to use.

B. How technology perpetuates P2P fraud and theft.

Fraudsters have extraordinary creativity;[24] they are constantly developing creative ways to steal people's money by setting up increasingly sophisticated schemes to obtain access to accounts or to fraudulently induce consumers into payment transactions.[25] The Federal Communication

---

[20] The FTC designates Zelle transfers as part of the "bank transfer or payment" category, which also includes bank-to-bank wire transfers. *See* Section IV.A of this testimony for FTC statistics on "bank transfer or payment," also available at https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/PaymentContactMethods.

[21] Cowley, Stacy and Nguyen, Lananh, "*Senators question Zelle over how it is responding to reports of rising fraud*," New York Times (Apr. 26, 2022), available at https://www.nytimes.com/2022/04/26/business/zelle-fraud.html.

[22] Pradelli, Chad, "*'I still don't know how they got access': Woman loses thousands after thief targets her Zelle app*," ABC Action News, WMPVI-TV Philadelphia, PA (Jun. 2, 2023), available at https://6abc.com/zelle-peer-to-peer-payment-apps-theft-auto-payments/13335405/.

[23] *See* CBS This Morning, "*Complaints against mobile payment apps like Zelle, Venmo surge 300% as consumers fall victim to more money scams*," CBS News (June 23, 2021), available at https://www.cbsnews.com/news/venmo-payal-zelle-cashapp-scams-mobile-payment-apps/ .

[24] *See* NCLC, EPIC report *Scam Robocalls: Telecom Providers Profit*, at 6-10 (Jun, 2022) available at https://www.nclc.org/wp-content/uploads/2023/02/Robocall-Rpt-23.pdf for examples of the types of scams utilized by robocalls and scam texts; *see also* Testimony of Margot Saunders, NCLC *"Protecting Americans from Robocalls,"* Hearing Before the U.S. Senate Committee on Commerce, Science & Transportation (Oct. 24, 2023) available at https://www.nclc.org/wp-content/uploads/2023/10/Testimony-of-NCLC-on-Robocalls-2023.pdf.

[25] *See the latest scam warning below which also involves impersonation of law enforcement.*

SCAM OF THE WEEK:
This Fake App Takes the Cake

Commission's (FCC) website includes a Scam Glossary detailing dozens of different ways individuals and small businesses have lost money to these schemes, [26] and the FCC specifically identified P2P apps as a primary means for executing scams and fraud.[27] Clearly, the warnings provided by the payment apps themselves to beware of scams and fraud are not adequate to protect consumers from the losses.

This recent scam is impressively complex. The cybercriminals start by impersonating law enforcement officers. They contact you, claiming that your bank account may have been involved in financial fraud. You're then asked to download a mobile app to help them investigate further. If you download the app, the cybercriminal walks you through the steps to set this scam in motion.

First, you are given a case number. When you search for that number in the app, you'll find legal-looking documents with your name on them. These documents make the scam feel more legitimate. Once your guard is down, the app asks you to select your bank from a list and then enter your account number and other personal information.

The most clever part of this scam is what the app does in the background. When you first install the app, it blocks all incoming calls and text messages. That way, you won't be alerted if your bank attempts to contact you about unusual behavior on your account. If all goes as planned, the cybercriminals will steal your money and sensitive information before you know what happened.

No matter how advanced the app is, you can stay safe from scams like this by following the tips below.

- Only download apps from trusted publishers. Anyone can publish an app on official app stores or sites—including cybercriminals.
- Be cautious of scare tactics that play with your emotions. Cyberattacks are designed to catch you off guard and trigger you to reveal sensitive information.
- If you're contacted by someone claiming to be in a position of authority, like law enforcement, ask them to confirm their identity. Real officials will understand your concerns and can provide information that doesn't require you to download an app.

The KnowBe4 Security Team

KnowBe4.com

[26] Federal Commc'ns Comm'n, Scam Glossary, *available at* https://www.fcc.gov/scam-glossary.
[27] Federal Commc'ns Comm'n, *As More Consumers Adopt Payment Apps, Scammers Follow* (updated Feb. 25, 2021), available at https://www.fcc.gov/more-consumers-adopt-payment-apps-scammers-follow.

Additionally, with imposter scams topping the FTC's category of fraud type in 2022,[28] the use of deep fakes generated by artificial intelligence (AI) to perpetuate payment fraud is disconcerting.[29] NCLC joined numerous nationwide and state advocacy organizations in sending a letter to the FTC and the CFPB on the threat of AI-generated deep fakes used for financial fraud.[30]

C. Current ambiguity in the law leaves consumers insufficiently protected from P2P fraud.

The Electronic Fund Transfer Act (EFTA) and its implementing Regulation E protect consumers when problems with electronic funds transfers, such as P2P transactions, occur. The law provides consumers with remedies for P2P fraud when it is unauthorized, such as when a criminal defrauds a person into turning over account credentials and then the criminal commits an unauthorized transfer. The definition of "unauthorized transfer" under Regulation E is a transfer from a consumer's account "initiated by a person *other than the consumer* without actual authority to initiate the transfer and from which the consumer receives no benefit."[31]

However, the response to consumer complaints about unauthorized payments by some of the largest players in the P2P market is inconsistent at best and possibly non-compliant.[32] It is unfortunately too common for financial institutions to fail to comply with the unauthorized use protections of the EFTA and deny reimbursement on improper grounds.[33]

The response to P2P payment fraud becomes even more problematic when it involves claims of

---

[28] *See* Federal Trade Commission, *New FTC Data Show Consumers Reported Losing Nearly $8.8 Billion to Scams in 2022,* (press release) (Feb. 23, 2023), available at https://www.ftc.gov/news-events/news/press-releases/2023/02/new-ftc-data-show-consumers-reported-losing-nearly-88-billion-scams-2022.

[29] *See* U.S. Department of Homeland Security, *Increasing Threat from Deepfake Identities*, 2021, available at https://www.dhs.gov/sites/default/files/publications/increasing_threats_of_deepfake_identities_0.pdf; Schwartz, Christopher and Wright, Matthew, "*Voice Deepfakes Are Calling. Here's How to Avoid Them*," Gizmodo (March 24, 2023) available at https://gizmodo.com/ai-deepfake-voice-how-to-avoid-spam-phone-calls-1850245346.

[30] NCLC *et al*., Letter to CFPB and FTC on Threat of AI-Generated Deep Fakes Used for Financial Fraud, available at https://www.nclc.org/wp-content/uploads/2023/10/Deepfake-based-financial-fraud-letter-to-CFPB-and-FTC.pdf.

[31] 12 C.F.R. § 1005.2(m) (emphasis added).

[32] Brown, Sherrod, Elizabeth Warren, and Jake Reed, "*Brown, Reed, Warren Urge Venmo, Cash App to Reimburse Victims of Fraud and Scams | United States Committee on Banking, Housing, and Urban Affairs*," (Dec. 14, 2023) available at https://www.banking.senate.gov/newsroom/majority/brown-reed-warren-urge-venmo-cash-app-to-reimburse-victims-of-fraud-and-scams. *See also* Hindenburg Research Report, "*Block: How Inflated User Metrics and 'Frictionless' Fraud Facilitation Enabled Insiders to Cash Out Over $1 Billion,*" (March 23, 2023), available at https://hindenburgresearch.com/block/.

[33] *See, e.g.,* CFPB, Supervisory Highlights at 17 (Summer 2022) ("Examiners continued to find issues with financial institutions failing to follow Regulation E error resolution procedures…. A financial institution cannot require a consumer to file a police or other documentation as a condition of initiating or completing an error investigation.); CFPB, Supervisory Highlights at 15 (Summer 2021), available at www.consumerfinance.gov (stating that "Supervision continues to find violations of EFTA and Regulation E that it previously discussed in the Fall 2014, Summer 2017, and Summer 2020 editions of Supervisory Highlights, respectively," (Listing several violations)); Sonbuchner, Scott, Examiner, Fed. Reserve Bank of Minneapolis, Consumer Compliance Outlook, Error Resolution and Liability Limitations Under Regulations E and Z; Regulatory Requirements, Common Violations, and Sound Practices (2d issue 2021), available at www.consumercomplianceoutlook.org.

fraudulently induced payments. P2P apps disclaim responsibility to protect consumers from fraudulently induced transactions, even though those payments go to accounts held at the same P2P app. Similarly, most banks will deny a claim of error for a fraudulently induced transaction, though Zelle has begun reimbursing consumers for some fraudulently induced transactions resulting from certain types of imposter scams.[34]

The definition of "unauthorized transfer" under Regulation E as described above contemplates a transaction that was not initiated by the consumer. If the consumer initiated the transfer, even if the consumer was defrauded into initiating the payment, financial institutions are likely to dispute their liability and may even refuse to help.

Nevertheless, some fraudulently induced transactions may fall under Regulation E's separate error protections, such as the protection against incorrect transactions – i.e., a payment that went to an imposter – or the right to obtain information.[35] The CFPB also has authority to define additional categories of error.[36]

The disparity of treatment between unauthorized and fraudulently induced payments under Regulation E is made clear in the following two scenarios:

- *Scenario A: Laurie receives a call from a person claiming to be with the IRS. The caller threatens to arrest her if she does not make a payment. Laurie gives the caller her bank account number and routing number, and the caller uses that information to initiate a preauthorized ACH debit against her account.*
- *Scenario B: Laurie receives a call from a person claiming to be with the IRS. The caller threatens to arrest her if she does not make a payment. Laurie takes out her smartphone and sends a P2P payment to the number or email given by the caller.*

Though there is very little difference in these two scenarios, Regulation E protects Laurie in Scenario A where she can contest the debit as unauthorized. In Scenario B, financial institutions will take the position that Laurie is unprotected because she initiated the payment. The difference between how the payment was initiated in Scenario A and B does not make a scammer any more entitled to the money or make the scammer's bank any less responsible for banking a scammer.

D. Responsibility of receiving institutions.

As discussed earlier, payments often involve two institutions: the one that sent the payment (the consumer's institution in the P2P context) and the one that received it. While the EFTA governs only the responsibilities of the consumer's institution, other laws and network rules give the receiving institution obligations to prevent fraud.

Scenario A described above is unlikely to occur because scammers like the fake IRS caller would be deterred from using the ACH system. The ACH system vets and monitors who is

[34] Campisi, Natalie, "*Scammed Out Of Money On Zelle? You Might Be Able To Get It Back*," Forbes (Nov. 13, 2023), available at https://www.forbes.com/advisor/money-transfer/zelle-users-refunded-after-scams/.
[35] 15 U.S.C. § 1693f(f)(2), (6); 12 C.F.R. § 1005.11(a)((1)(ii), (vii).
[36] 15 U.S.C. § 1693f(f)(7).

allowed to initiate ACH payments, and the liability of a bank that initiates and receives fraudulent debit payments under both Regulation E and Nacha rules leads to stronger controls that are more likely to keep the scammer from having an account or having access to the ACH system.

But with the growth of payment apps, online bank account opening, and identity theft, it is easier for scammers to obtain accounts – potentially using stolen or synthetic identities – that they can then use to receive payments (directly or through money mules). Yet at present, the payment service or bank receiving the fraudulent payment on behalf of the scammer has no direct liability for enabling the scammer to receive the payment. As a result, that institution has less incentive to prevent the scammer from obtaining an account, put a hold on access to suspicious payments, or shut down the account quickly.

If consumers had more remedies against fraudulently induced transactions, payment network rules could pass liability in whole or in part back to the institution that holds the fraudster or money mule account, which would help to correct these incentives. This is what the United Kingdom has done, as discussed below.

Consumer complaints of P2P fraud will continue to escalate because the current systems impose insufficient responsibility on system operators and financial institutions to protect consumers against fraudulent schemes. Given what we know about how fraudsters target opportunities with the least resistance, it stands to reason that fraudulently induced payment fraud will continue to plague P2P systems if payment systems and financial institutions are allowed to operate under the assumption that they are not liable.

E. Problems with P2P apps when consumers make mistakes.

Beyond fraudulently induced payments and unauthorized payments, P2P payment apps and financial institutions typically refuse to help consumers who accidentally send money to the wrong person or the wrong account – mistakes that are easy to make in payment services designed for convenience and speed over safety. For example, consumers can send money through P2P systems using nothing more than a cell phone number to identify the recipient.

Here are other examples:

- An employee of NCLC unexpectedly saw $1,000 arrive in his bank account through Zelle. A few minutes later, he received a frantic phone call from a man telling him that he had put in the wrong cell phone number and asking for the money back. The NCLC employee wanted to return the money but asked his bank for assurances that it was not a scam. The man also called his bank. Both banks (each large top-10 institutions) refused to help correct the error. After weeks of getting nowhere, the NCLC employee returned the funds on faith.

- Arthur Walzer of New York City tried to send his granddaughter $100 through Venmo as a birthday present, but instead sent it to a woman with the same first and last name. When he discovered the error, he told his bank to refuse payment of the $100, and in response

> Venmo froze his account and demanded that he pay them. Venmo eventually refunded him, but only after a journalist contacted the company on his behalf. It was the first time he had ever used Venmo – he set up an account specifically to give his granddaughter the gift.[37]

Regulation E imposes the duty to investigate and resolve "errors," which includes "an incorrect electronic fund transfer to or from the consumer's account."[38] Nothing in the EFTA excludes consumer errors, and Regulation E should be interpreted to cover them. When a payment is sent to the wrong person or in the wrong amount, the person receiving the payment is not more entitled to the payment because the error was caused by the sender. But today, most consumers are out of luck in this situation unless their bank decides to help and the receiving bank or payee is cooperative.

F. Potential remedies to address P2P payment fraud.

1. Update the Electronic Funds Transfer Act.

The EFTA was enacted 43 years ago and as described above does not directly address many of the most important issues in the current consumer payment ecosystem. The statute was initially adopted at a time when consumers were conducting business with their own financial institutions and were using payment systems that did not lead to the same types of problems that plague today's P2P systems.

We support legislative efforts to address the many gaps and ambiguities in the Electronic Fund Transfer Act that leave consumers unprotected. Some of these problems could also be addressed by rulemaking or guidance from the CFPB, though Congressional action would be faster and less subject to challenge.

The problem of fraudulently induced electronic transfers in P2P payments could be addressed by amending the EFTA to protect consumers from liability when they are defrauded into initiating a transfer and allow the consumer's financial institution, after crediting the consumer for a fraudulent transfer, to be reimbursed by the financial institution that allowed the scammer to receive the fraudulent payment.

Problems when consumers make mistakes could also be addressed by clarifying that the EFTA's error resolution procedures apply when the consumer makes a mistake, such as in amount or recipient.

2. Consider the United Kingdom as an example.

The United Kingdom (UK) was early to launch real time payments, and fraudulently induced payment fraud (what the UK calls authorized push payment or APP fraud) immediately

---

[37] *See* Elliott, Christopher, "*A Venmo user sent $100 to the wrong person. Then the payment service froze his account*," Seattle Times (Nov. 2, 2020), available at https://www.seattletimes.com/life/travel/a-venmo-user-sent-100-to-the-wrong-person-then-the-payment-service-froze-his-account-travel-troubleshooter/.

[38] 15 U.S.C. § 1683f(f)(2); 12 C.F.R. § 1005.11(a)(1)(ii).

followed. The UK has been formally considering how to tackle the problem of P2P fraud since 2016, when the consumers association "Which?" submitted a "super-complaint"[39] to the United Kingdom's Payments Systems Regulator (PSR).[40] The complaint identified the problem of APP fraud, which happens when scammers deceive consumers or individuals at a business to send them payment under false pretenses to an account controlled by the scammer. Which? also identified the lack of consumer protection for victims of APP fraud.

In response, a steering group was formed, comprised of regulators, consumer advocates, financial services providers and industry representatives.[41] The result was the creation of an industry code called the Contingent Reimbursement Model (CRM) Code, launched in 2019. The CRM Code required signatories to reimburse consumers who were the victims of APP fraud under certain circumstances.[42] The CRM Code was voluntary and existed to help financial institutions in the UK, "detect, prevent and respond to APP scams."[43]

The voluntary decision of the leading UK payment industry players to develop a system to reimburse fraud victims shows the consensus that protecting consumers benefits industry players and the payment systems as a whole, not merely consumers. But the uneven implementation of the system – and the growing calls to make it mandatory – also show the limits of voluntary measures.

As reported in September 2021, very few victims of APP fraud were reimbursed under the CRM Code: "banks found victims at least partly responsible in 77% of cases assessed in the first 14 months following the introduction of a Contingent Reimbursement Model and voluntary code."[44] Two banks found the customer fully liable in 90% of their decisions.[45]

Under the CRM code, consumers who were unhappy with their bank's refusal to compensate them could appeal to the Financial Ombudsman Service, which reviewed denials of reimbursement requests for APP fraud. Data obtained by Which? found that in 73% of the complaints the ombudsman received about APP fraud from 2020-2021, the ombudsman concluded that banks were getting the decisions wrong, reversed the banks' denials, and found in

---

[39] A super-complaint may be made by a designated consumer body where the body considers features of a market in the United Kingdom for payment systems that are or which may be significantly damaging to the interests of consumers. https://www.gov.uk/government/publications/super-complainants-for-the-payment-systems-regulator.

[40] As part of the Financial Services (Banking Reform) Act of 2013, the Payment Systems Regulator (PSR) was established to promote competition, innovation, and responsiveness of payment systems and to receive and respond to super-complaints. https://www.gov.uk/government/publications/super-complainants-for-the-payment-systems-regulator.

[41] Speech by the Lending Standards Board Chief Executive, Emma Lovell, "*International Perspective-Scams: Looking Forward: Priorities and opportunities*," (Mar. 15, 2022) available at https://www.lendingstandardsboard.org.uk/scams-looking-forward-priorities-and-opportunities-international-perspective-speech/.

[42] *Id.*

[43] *Id.*

[44] "*Banks called to account over 'shockingly low' rate of reimbursements for APP fraud*," Finextra (Sept. 15, 2021) available at https://www.finextra.com/newsarticle/38832/banks-called-to-account-over-shockingly-low-rate-of-reimbursements-for-app-fraud

[45] *Id.*

favor of the consumer.[46] This level of reversals suggests that the banks' high rate of denials was inconsistent with both the letter and the spirit of the Code.[47]

The Contingent Reimbursement Model as an industry response, though laudable and necessary, proved insufficient to address the growing number of scams and fraud. In the first half of 2021, APP fraud cases in the UK outnumbered credit card fraud for the first time.[48]

Consequently, the UK Parliament's Treasury Committee recommended "mandatory refunds" to victims of APP fraud and discussion about whether to make "big technology companies liable to pay compensation when people are tricked by con-artists using their platforms."[49] As a result, the Payment Systems Regulator (PSR) undertook rulemaking, subject to a period of open comment ("consultation").

In June 2023, the PSR finalized a rule that requires mandatory reimbursement to victims of APP fraud.[50] Under the finalized rule, the victim's financial institution and the recipient's financial institution split the cost of reimbursement 50:50.[51]

3. When liability is split between sending and receiving institutions and not pushed onto consumers, more will be done to protect consumers.

P2P apps must take more responsibility to protect consumers from the fraud committed on their platforms and from the scammers they allow to open accounts where they can receive stolen funds.[52] While consumer education is important and necessary, payment system providers' primary response to fraud and errors in P2P systems should not be to use old-fashioned disclosures and warnings to consumers to "be careful" and not to send payments to people they do not know—all while promoting their systems for broad use. Scammers prey on consumers' trust, and warnings are far less effective than sophisticated systems that payment providers can design.

The providers of P2P payment apps and payment systems as well as the financial institutions

---

[46] Which?, "*Banks wrongly denying fraud victims compensation in up to 8 in 10 cases*," (Nov. 11, 2021), available at https://www.which.co.uk/news/2021/11/banks-wrongly-denying-fraud-victims-compensation-in-up-to-8-in-10-cases/.

[47] Contingent Reimbursement Model Code for Authorised Push Payment Scams OP1 at 2, (Apr. 20 2021), https://www.lendingstandardsboard.org.uk/wp-content/uploads/2022/03/CRM-Code-LSB-April-2021.pdf

[48] "*UK Government to Legislate for Mandatory Reimbursement of App Fraud*," (Nov. 18, 2021), available at https://www.finextra.com/newsarticle/39245/uk-government-to-legislate-for-mandatory-reimbursement-of-app-fraud

[49] "*Fraud: MPs seek overhaul to tackle financial scammers*," (Feb. 2, 2022), available at https://www.bbc.com/news/business-60216076.

[50] Press Release: "*PSR confirms new requirements for APP fraud reimbursement*," available at https://www.psr.org.uk/news-and-updates/latest-news/news/psr-confirms-new-requirements-for-app-fraud-reimbursement/.

[51] To view a summary of the new rule and the feedback received during the open consultation, go to https://www.psr.org.uk/media/iolpbw0u/ps23-3-app-fraud-reimbursement-policy-statement-final-june-2023.pdf.

[52] *See* Sanchez-Adams, Carla, "*It is essential that we protect consumers from fraud over P2P networks,*" American Banker, Bank Think (Mar. 15, 2023), available at https://www.americanbanker.com/opinion/it-is-essential-that-we-protect-consumers-from-fraud-over-p2p-networks.

who utilize these applications make decisions about what safety features to install, when to protect consumers, and how to monitor and react to red flags of potentially fraudulent payments sent and received by their customers. Companies that are incentivized to prevent fraud and errors will use constantly improving technology and innovations to spot potential scams and errors and to aggregate reports of fraud. Because the UK's new rule will require financial institutions to compensate consumers affected by fraudulently induced transfers (APP scams), for example, nine of the UK's biggest banks have signed up to use a new AI-powered tool that helps banks more effectively spot if their customers are sending money to fraudsters.[53]

Furthermore, financial institutions already have "Know Your Customer" (KYC) and account monitoring obligations under the Bank Secrecy Act (BSA) and Anti-Money Laundering (AML) laws, which should be reflected through their Customer Identification Program (CIP) and Customer Due Diligence (CDD) policies. Even P2P payment apps and fintech companies have certain obligations under the BSA. To comply with these laws, the institutions make decisions about who they allow to open an account and how to monitor and react to red flags of potentially fraudulent payments sent and received by their customers. When they fail in those responsibilities and allow a customer to use an account to receive stolen funds, it is appropriate for that institution to bear the costs if the funds cannot be recouped.

If fraud and error rates are low in the aggregate, the system can bear those costs and spread them. If rates are high, then the systems clearly have fundamental problems that must be addressed. But even a single instance of fraud or mistake can be devastating to a consumer. The equities strongly favor protecting consumers with the same type of strong protection they have in the credit card market.

4. Address the lack of oversight for certain parties involved in the payments market.

Newer fintech companies, including technology providers and payment apps, do not receive the same type of supervision as other financial institutions in the United States. But the CFPB has proposed a rule that will enable it to supervise large market participants who provide general-use digital consumer payment applications.[54] Greater supervision is important because compliance with basic EFTA obligations has been problematic even in supervised financial institutions, as noted above. The CFPB should swiftly finalize that rule and expand it to encompass the larger participants on the debit and prepaid card markets and domestic money transfer markets as well.

---

[53] Solon, Olivia "*Nine British Banks Sign Up to New AI Tool for Tackling Scams*," Bloomberg (Jul. 25, 2023) available at https://www.bloomberg.com/news/articles/2023-07-05/mastercard-s-ai-tool-helps-nine-british-banks-tackle-scams.

[54] The CFPB issued a proposed rule to define larger participants of a market for general-use digital consumer payment applications which closed on January 8, 2024. The proposed rule may lead to greater supervision of some nonbank payment services, though not all. *See* NCLC *et al*., Comments to the CFPB's Proposed Rule Defining Larger Participants of a Market for General-Use Digital Consumer Payment Applications, (Jan. 8, 2024) available at https://www.nclc.org/wp-content/uploads/2024/01/240108-CFPB-Payments-App-Comment-Final.pdf.

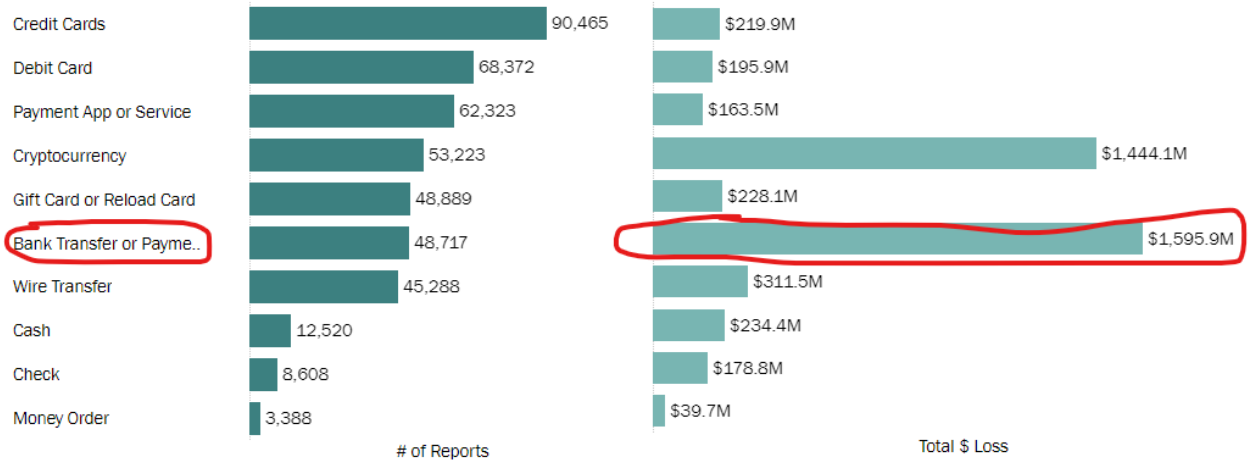
IV. Bank-to-Bank Wire Transfer Fraud.

A. Consumers are devastated by bank-to-bank wire transfer fraud.

The FTC's latest fraud data show that, in terms of dollars lost, "Bank Transfer or Payment" is the largest payment method used by fraudsters.[55] It also seems safe to assume that the lion's share of those losses by dollar volume are through bank-to-bank wire transfers, which can process very large transfers, rather than through Zelle. (The FTC's "Wire Transfer" category includes only nonbank transfers like Western Union and MoneyGram.)

Cryptocurrency is a close second to bank transfer in total dollar amount of fraud losses reported to the FTC, and some losses through cryptocurrencies may start as bank-to-bank wire transfers to crypto banks or exchanges.[56] For example, Marjorie Bloom of Chevy Chase, Maryland, a 77-year-old retired civil servant, lost her life savings, $661,000, through a bank-to-bank wire transfer into cryptocurrency.[57]

2022 Fraud Reports to FTC by Payment Method



Compared to 2019, it is especially dramatic to note how the bank transfer category has overtaken nonbank wire transfers, and how astronomically it has grown – nearly ninefold in five years.[58]

2019 Fraud Reports to FTC by Payment Method

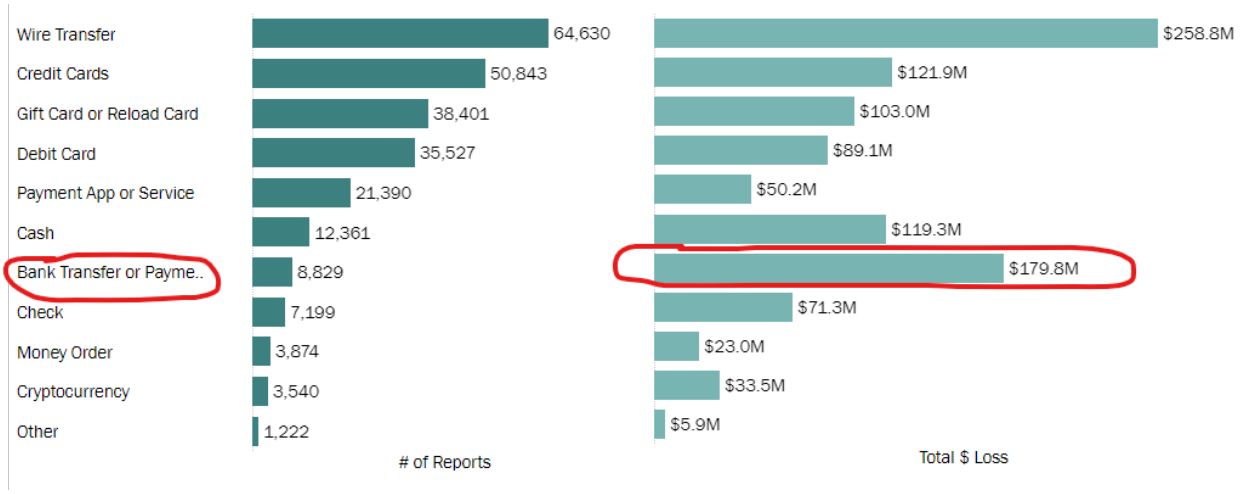
---

[55] FTC fraud reports by payment method available at https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/PaymentContactMethods.

[56] *See* Paluska, Michael, "*Cryptocurrency scam drains retired St. Pete victim's life savings How to spot online scams*," ABC Action News (Florida) (June 19, 2023), available *at* https://www.abcactionnews.com/news/region-pinellas/cryptocurrency-scam-drains-retired-st-pete-victims-life-savings.

[57] Iacurci, Greg, "*How this 77-year old widow lost $661,000 in a common tech scam: 'I realized I had been defrauded of everything'*," CNBC (Oct. 8, 2023) available at https://www.cnbc.com/2023/10/08/how-one-retired-woman-lost-her-life-savings-in-a-common-elder-fraud-scheme.html.

[58] The dollar losses in these two charts significantly understate actual losses, as only 12% (2019) to 17% (2022) of reports included information on payment method, and many fraud losses are not reported to the FTC.



For the first three quarters of 2023, the dollar amount of fraud losses due to bank transfer or payment reported to the FTC are on pace to exceed 2022 dollar losses by 14%.[59]

Over the last several years, NCLC has received numerous inquiries on behalf of consumers and heard devastating reports about how criminals have used bank-to-bank wire transfers to take

hundreds of thousands of dollars from people. In one case, an older woman lost her home as a result. Here are other examples:

- A college student lost his entire savings account after someone with two fake identification cards went into a bank and wired $16,500 to another individual. Busy with college, he did not notice missing money for a month and a half, but the bank refused to return the money.[60]

- After a consumer was the victim of a SIM swap, a wire transfer was used to transfer $35,000 from his bank account to an account in another state.[61] He is a cancer patient and navigating the bank appeal process has been extremely stressful. These SIM swaps are increasingly common.[62]

- A low-income consumer in New York lost over $26,000 – all her savings, which she had carefully saved over many years – after someone transferred money from her savings account to her checking account and then made an outgoing wire transfer to another state.[63]

- A man lost $15,000 that was wired to another account by someone who gained access to his account. The bank spotted suspicious activity as the fraud was taking place and

[59] FTC fraud reports by payment method available at https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/PaymentContactMethods.
[60] Inquiry received by KPRC (Houston NBC station) reporter Amy Davis.
[61] Email from attorney on file with NCLC.
[62] *See* Barr, Luke, ABC News, "*'SIM swap' scams netted $68 million in 2021: FBI*" (Feb. 15, 2022), available at https://abcnews.go.com/Politics/sim-swap-scams-netted-68-million-2021-fbi/story?id=82900169.
[63] Email from CAMBDA Legal Services to NCLC, on file with NCLC.

called the man, who alerted them to the fraud, but the bank still refused to return the money claiming that the EFTA did not apply to these fraudulent electronic transactions.

- A fraudster hacked a retiree's online banking account and made a cash advance from the retiree's credit card to his linked bank account. The fraudster then immediately wired that amount from the retiree's bank account to his own. The bank denied any relief.[64]

- A small business had its online banking account hacked and its $60,000.00 checking account balance emptied over the course of two days and six transactions. The bank denied relief because its banking agreement generally states that customers are responsible for unauthorized transactions.[65]

Wire fraud has become so problematic that even large news outlets like Good Morning America have run stories about the perils and lack of protection available to impacted consumers.[66]

All the examples provided above were for unauthorized wire transfers. However, we have also heard stories where the consumer was fraudulently induced into sending a wire transfer. For example:

- Three Ohio residents were all defrauded into making a bank-to-bank wire transfer by a Chase impersonation scam.

    - Jeff Phipps from Columbus, Ohio lost $8,500 after the fraudster, impersonating a bank employee, called and convinced the man that his account had been hacked into and he needed to provide login information to protect it. "They asked him if he had authorized a wire transfer and he replied, 'no'. They kept him on the phone for an hour and 47 minutes. They said, 'Well, we want to deactivate your account. Can you send us your username and your passcode?' And he did thinking it was Chase." The fraudster took $8,500 with this information and Chase refused to refund the victim's money since he had given information to the scammer, "authorizing" it.[67]
    - Kelli Hinton, 7 months pregnant at the time, received a text about a fraudulent wire transfer from her account, then a follow-up call from a fraudster posing as a Chase fraud agent, spoofing Chase's real phone number. The fraudster kept her on the line for an hour and convinced her to change her username and

[64] Pending arbitration before AAA (Wells Fargo).
[65] Lawrence and Louis Company d/b/a Hidden Oasis Salon v. Truist Bank, No. 1:22-cv-200-RDA-JFA (E.D. Va.).
[66] ABC News, Good Morning America "*Woman sounds alarm on sophisticated wire transfer fraud*," (Jul. 21, 2023), available at https://abcnews.go.com/GMA/Living/video/woman-sounds-alarm-sophisticated-wire-transfer-fraud-101547100.
[67] Gordon, Clay, "*Central Ohio man loses $8,500 in Chase bank impersonation scam*," 10 WBNS (Mar. 30, 2023), available at https://www.10tv.com/article/money/consumer/wire-fraud-scam-warning/530-7af76f5c-cce0-4dcc-98a3-5c740a9043bd.

password, allowing him to drain $15,000 from her account.[68]

- Just months after experiencing a near fatal collision that left him in a wheelchair, Todd Evans from West Chester Township was called by a fake Chase fraud protection agent. The fraudster told him about a fraudulent purchase from his account, which Todd confirmed was appearing on his account and which neither he nor his wife had made. The fraudster then mentioned a $45,000 fraudulent wire transfer from the account. Todd and his wife were nervous about addressing the fraud and asked the caller to verify his identity. He asked the couple to look at the number he was calling from and verify it matched the number on their debit card. Based on this confirmation, the couple allowed the fraudster to guide them through a "wire reversal process". Hours later they were out $63,000.[69]

- A couple in South Carolina received an email from their attorney at the time of closing their home purchase with instructions on where to send the down payment via bank-to-bank wire transfer. Their attorney had been the victim of a phishing scam, and the fraudster used a legitimate email copying an actual employee of the attorney. The couple lost $108,000.[70]

Even in instances where consumers realize they have fallen prey to a fraud scheme, banks are sometimes unwilling or unable to assist consumers or stop a wire transfer. For example, Ann Booras from San Ramon, California received a call from a fraudster impersonating a Wells Fargo employee asking if she had wired $20,000 from her savings account. In response to the directions provided by the fake employee, Ann wired the $20,000 sum to the "bank's fraud department" where it would be safe. The fraudster then continued asking about other supposedly fraudulent transactions, and panicking, Ann "drove to the nearest Wells Fargo branch, with the man still on the phone, and told a teller someone was attacking her accounts. Silently, the teller warned her - the thief was actually the man on the phone. 'I had tears running down my face, I was literally shaking because I realized I had just sent $25,000 to who knows where,'." Ann "pleaded with bank employees to stop those wire transfers -- fast. But to her shock, no one would help." She was told, "I'm sorry we're all busy. We're backed up with appointments back to back. You need to go to another branch, but we can't help you here."[71]

B. Technology enables more bank-to-bank wire transfer fraud.

---

[68] McCormick, Erin "*Gone in seconds: rising text scams are draining US bank accounts*," The Guardian (Apr. 22, 2023), available at https://www.theguardian.com/money/2023/apr/22/robo-texts-scams-bank-accounts.

[69] Johnson, Karin "*West Chester couple swindled out of thousands of dollars by crooks spoofing bank's phone number*," WLWT5 news (Nov. 16, 2023), available at https://www.wlwt.com/article/west-chester-chase-bank-spoofing-phone-number/45866051.

[70] Lee, Diane, "*Upstate couple warns of wire fraud that cost them $108,000*," CBS7 News, (May 19, 2023), available at https://www.wspa.com/news/upstate-couple-warns-of-wire-fraud-that-cost-them-108000/.

[71] Finney, Michael and Koury, Renee, "*Wells Fargo bankers tell East Bay customer they're too busy to stop wire scam*," ABC7 (Jun. 21, 2023), available at https://abc7news.com/bank-impostor-scam-wells-fargo-wire-transfer-fraud-scammer-pretends-to-be/13407340/#:~:text=Wells%20Fargo%20bankers%20tell%20East,busy%20to%20stop%20wire%20scam&text=The%20victim%20was%20still%20on,SAN%20RAMON%2C%20Calif.

As the previous stories all illustrate, fraudsters have taken advantage of the technology needed to send texts and make calls to consumers whose information has been obtained through phishing schemes or purchased from the dark web. Technology also enables fraudsters and hackers the ease to take over accounts and initiate transactions through online or mobile banking.

Previously, wire transfers had to be conducted through a cumbersome process of walking into a bank for a time-consuming, in-person transaction. In-person identification would prevent unauthorized transfers, and there were some speed bumps for fraudulently induced transactions as well—the consumer would have time to think about the situation, call a family member, and talk to the bank teller, who could potentially talk them out of it.

But increasingly, bank-to-bank wire transfers are a service offered and permitted through mobile and online banking. As a result, fraudsters have an easy method of using unauthorized or fraudulently induced transfers to steal and send large sums of money, often not possible through P2P apps that set daily transaction limits. The lack of friction that was found in in-person transactions has undoubtedly contributed to the explosion of bank-to-bank wire transfer losses.

C. Bank-to-bank wire transfers are exempt from the EFTA, leaving consumers exposed to losing thousands of dollars.

The EFTA exempts electronic transfers, other than ACH transfers, made "by means of a service that transfers funds held at either Federal Reserve banks or other depository institutions and which is not designed primarily to transfer funds on behalf of a consumer."[72] Regulation E and the official interpretations of Regulation E interpret that exemption to cover wire transfers using FedWire, SWIFT, CHIPS, and Telex.[73] Thus, even if a criminal impersonates the consumer and makes a completely unauthorized wire transfer, the consumer may have no protection under Regulation E.[74]

At the time the EFTA was written in 1978, bank-to-bank wire transfer services were not viewed as a consumer payment system. That has clearly changed— bank-to-bank wire transfer services are now incorporated into consumer mobile and online banking services and electronic fund transfers are generally far more common among consumers today than in 1978. For large payments, bank-to-bank wire transfers are the primary way consumers can conduct electronic transfers.

Instead of the clear consumer protections provided by the EFTA, which was designed to protect consumers with clear rights and procedures, bank-to-bank wire transfers are covered under state law, more specifically a state's adopted version of Uniform Commercial Code Article 4A (UCC Article 4A). The UCC was not designed as a consumer protection statute and was instead

---

[72] 15 U.S.C. §1693a(7)(B).
[73] 12 C.F.R. §1005.3(c)(3) (exempting FedWire or similar systems); Official Interpretation of 3(c)(3)-3 ("Fund transfer systems that are similar to Fedwire include the Clearing House Interbank Payments System (CHIPS), Society for Worldwide Interbank Financial Telecommunication (SWIFT), Telex, and transfers made on the books of correspondent banks.").
[74] However, as discussed in FN 77 below, some bank wire transfers may be within the EFTA's protection.

designed to govern commercial-to-commercial transactions. UCC Article 4A offers very weak or no protection for consumers who have suffered harm due to bank-to-bank wire transfer fraud. In essence, the consumer is deemed to have authorized a wire transfer if the bank utilized a commercially reasonable security procedure that the bank and the consumer agreed to beforehand and if the bank acted in good faith. Yet consumers have no understanding of or control over those security procedures and no choice but to click "I agree" to the fine print of an agreement.

For example, the New York Attorney General recently filed a lawsuit against Citibank alleging it failed to protect and reimburse victims of electronic fraud when it used "poor security and anti-fraud protocols," that consumers had not negotiated with Citibank.[75] According to the lawsuit, Citibank connected wire transfer services to consumers' online and mobile banking apps in recent years— allowing direct electronic access to the wire transfer networks— but employed lax security protocols and procedures; had ineffective monitoring systems; failed to respond in real-time; and failed to properly investigate fraud claims.[76] As a result, New Yorkers lost millions of dollars in life savings, their children's college funds, and even money needed to support their day-to-day lives.

I have also heard numerous other reports of banks failing to reimburse unauthorized wire transfers even if the consumer did not agree to any commercially reasonable security procedure. Consumers do not have the resources to fight the bank in court or arbitration to enforce their right to a reimbursement when this occurs.

UCC Article 4A does not provide a consumer with any other remedies besides reimbursement (and possible interest) of the unauthorized wire amount, and the consumer's attorney is not entitled to recover attorneys' fees from the bank. As a practical matter, it means that a consumer would have to pay out of pocket to fight in court or in arbitration just to get their money back, while a financial institution with deep pockets can afford to fight a claim. As a result, in most cases financial institutions will reject a consumer's unauthorized wire transfer claim because the consumer cannot afford to fight the decision.

With respect to fraudulently induced wire transfers, the UCC provides no remedy.

D. Potential remedies to address bank-to-bank wire fraud.

As previously stated, we support legislative efforts to address gaps in the Electronic Fund Transfer Act that leave consumers unprotected.

The EFTA can be amended to address specific problems of unauthorized consumer bank-to-bank

[75] New York State Attorney General, Press Release, Attorney General James Sues Citibank for Failing to Protect and Reimburse Victims of Electronic Fraud (Jan. 30, 2024), *available at* https://ag.ny.gov/press-release/2024/attorney-general-james-sues-citibank-failing-protect-and-reimburse-victims.

[76] *See* Complaint, People of the State of New York v. Citibank, No. 1:24-cv-00659 (S.D.N.Y. filed Jan. 30, 2024), *available at* https://ag.ny.gov/sites/default/files/2024-01/citi-complaint.pdf. The New York AG also alleges that the unauthorized wire transfers that occurred by electronic requests initiated by scammers via online banking or mobile app are covered by the EFTA. They are electronic instructions that do not come from the actual consumers who are Citi account holders and under the EFTA are unauthorized.

wire transfers as well as fraudulently induced consumer bank-to-bank wire transfers by:

- Eliminating the exemption for bank wire transfers and electronic transfers authorized by telephone call, bringing those transfers within the EFTA and its protections against unauthorized transfers and errors;
- Protecting consumers from liability when they are defrauded into initiating a transfer, and
- Allowing the consumer's financial institution, after crediting the consumer for a fraudulent transfer, to be reimbursed by the financial institution that allowed the scammer to receive the fraudulent payment.

The consumer bank-to-bank wire transfer loophole and inclusion of fraudulently induced transfers could also be addressed by rulemaking or guidance from the CFPB, though Congressional action would be faster and less subject to challenge.

V. Check Fraud.

A. Check alteration fraud is on the rise.

Although checks are an old payment system, new technology is leading to a rise in fraud using checks. In particular, new technology makes it easier for criminals who steal checks to engage in "check washing" – changing the payee and payment amount on a check – and harder for banks or consumers to spot those alterations.[77] Criminals can also create fake checks from stolen account information. These altered or fabricated checks can then be deposited remotely through mobile devices, made easier through the increased ability to open fraudulent accounts into which those checks can be deposited, as described in Section III.D above.

Although checks are near the bottom of payment types in terms of number of fraud reports, the total dollar loss by check fraud reported to the FTC is actually higher than for payment apps and services: $177.4 million in 2022 for checks compared to $163.5 million for payment apps and services. But this reported dollar loss is vastly understated;[78] one report a year ago puts annual check fraud losses at $815 million.[79]

Check fraud loss reported to the FTC increased by over 15% from 2021 to 2022.[80] Based on the first three quarters of 2023, check fraud losses are on pace to exceed 2022 numbers by 40%.[81]

In February 2023, FinCEN issued an alert about a nationwide surge in mail theft-related check fraud schemes and urged financial institutions to "be vigilant in identifying and reporting such

---

[77] DePompa, Rachel, '*Check washing' scams still on the rise*," Fox10 News (Jan. 25, 2024), *available at* https://www.fox10tv.com/2024/01/25/check-washing-scams-still-rise/.
[78] Of the 2.5 million reports of fraud received by the FTC in 2022, only 17% specified the payment method for the fraud. FTC fraud reports by payment method available at https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/PaymentContactMethods.
[79] Nadelle, David, "*Check Washing Is an $815M Per Year Scam — How It Works and Ways To Prevent It*," GoBanking Rates, (Feb. 22, 2023), https://www.nasdaq.com/articles/check-washing-is-an-$815m-per-year-scam-how-it-works-and-ways-to-prevent-it.
[80] *Id.*
[81] *Id.*

activity."[82] The report indicated that there were over 680,000 cases of possible check fraud reported to FinCEN in 2022 through the use of SARs (Suspicious Activity Reports), an increase from a little over 350,000 check fraud-related SARs sent to FinCEN in 2021, which itself was a 23% increase from 2020.[83] The statistics for check-fraud related SARs were not specific to mail-theft related check fraud.[84]

Technology also enables criminal organizations to traffic stolen checks. As a recent New York Times article[85] conveyed:

> "The cons may start with stealing pieces of paper, but they leverage technology and social media to commit fraud on a grander scale, banking insiders and fraud experts said. In the past, criminals needed a special internet browser that would grant entry into the dark web marketplace of stolen checks, maybe even someone to vouch for them. Now all they need is an account from Telegram, a messaging app.
>
> "You can buy checks on the internet for $45, with a perfectly good signature," said John Ravita, director of business development at SQN Banking Systems, which provides check fraud detection software. "There is one website that offers a money-back guarantee. It's like Nordstrom."

NCLC spoke with Larry Smith, an attorney in Chicago, whose clients did not even have checks issued to their associated bank account, yet a fraudster somehow obtained their bank account and routing number and created fake checks.[86] The fraudster deposited these checks in various bank accounts from December 2021 and January 2022, stealing around $14,000 from the consumers. Though the consumers disputed the fraudulent checks with their bank and have filed a lawsuit, their bank has not recredited their account for the stolen amount.

B. Though some protections exist for consumers harmed by check fraud, they are often left scrambling.

Checks are largely governed by state law through the Uniform Commercial Code (UCC). If a consumer timely reports the problem, the UCC protects them if their checks are altered or if a fraudulent check is presented against their account.[87]

Yet as the previous example demonstrates, consumers are often left scrambling, waiting for their banks to recredit their account even when state law provides remedies for the consumer when a

---

[82] FIN-2023-Alert003 available at https://www.fincen.gov/sites/default/files/shared/FinCEN%20Alert%20Mail%20Theft-Related%20Check%20Fraud%20FINAL%20508.pdf

[83] *Id. citing* FinCEN SAR Stats available at https://www.fincen.gov/reports/sar-stats

[84] *Id. See* FN 10.

[85] Barnard, Tara Seigel, "*We Can't Stop Writing Paper Checks. Thieves Love That*," (Dec. 9, 2023) available at https://www.nytimes.com/2023/12/09/business/check-fraud.html?unlocked_article_code=1.QU0.O8_m.7j3dyrD0mzvX&smid=url-share

[86] Arroyo and Ramos v. Fifth Third Bank, N.A., Cause No. 2023L004163, Cook County, IL.

[87] *See* U.C.C. §§ 3-407(b), (c) cmt. 2, 4-401(d)(1) for a consumer's rights when a check is altered; *see* U.C.C. §§ 4-401; 4-406(f) for a consumer's rights when a check is forged.

check is altered or forged. One consumer in Los Angeles was unable to get his account recredited for over two years. The consumer had written a check to the IRS and sent it by mail. The check was stolen from the mail and deposited into an account that was not the U.S. Treasury.[88] The consumer's bank kept insisting it would not recredit his account until the fraudster's bank sent them reimbursement.

While a bank's obligation to reimburse a consumer for an altered check is not dependent on the bank's ability to be repaid by the depository bank, the failure to timely resolve check fraud between institutions has also been the subject of complaint by community banks against their large-bank counterparts.[89] Consumers turn to their own bank for reimbursement when a check is altered or forged, and that bank in turn will request reimbursement from the bank into which the check was fraudulently deposited. As previously described in more detail in Section III. F. 3., the depository bank has "know-your-customer" responsibilities that are important to prevent fraud, but there is insufficient incentive to be diligent if there is no liability. As Steven Gonzalo, president and CEO of American Commercial Bank & Trust, stated: "From a deposit perspective, some banks do not perform the same level of due diligence because the bank assumes the risk of loss to them is zero or minimal, and fails to consider losses due to fraud incurred by the counterparty banks. And therein lies the failure."[90]

Furthermore, even though the UCC provides consumers up to a year to inform their bank of a fraudulent or altered check, it allows banks to shorten that notification time in the fine print of account agreements. Many bank account agreements shorten that time for notification to anywhere between 14 and 30 days.

Yet check alterations can be hard to spot. If the payee has been changed but not the amount, the consumer might have no reason to think that anything is amiss. For example, one consumer reported to NCLC that he had no idea his check had been altered until his landlord – a family friend – eventually told him months later that he had not received the rent.

Most banks no longer return physical checks to consumers and have also engaged in an aggressive push to eliminate paper statements. Bank websites and mobile apps focus on listing transactions but make it more cumbersome to review actual statements. The grainy photocopies of checks included with statements can be hard to read, consumers may not expect to have any reason to look at them, and those images are not even available to review on some mobile banking apps.

But if the consumer does not inform their bank about the check fraud before the end of the 14- to 30-day time period, they may be left with absolutely no recourse at all.

C. Potential remedies to address check fraud.

[88] *See* Lazar, Kristine, "*On Your Side: Check fraud is on the rise- here's how to protect your* money," CBS News Story, KCAL News (Apr. 17, 2023), available at https://www.cbsnews.com/losangeles/news/on-your-side-check-fraud-is-on-the-rise-heres-how-to-protect-your-money/.
[89] Berry, Kate, "*Small banks urge crackdown on big banks with lax check-fraud controls*," American Banker (Feb. 9, 2023), available at https://www.americanbanker.com/news/small-banks-urge-crackdown-on-big-banks-with-lax-check-fraud-controls
[90] *Id.*

To protect consumers from check fraud:

- Federal bank regulators should examine institutions to ensure that they are complying with their responsibility to reimburse consumers for altered or forged checks.
- Federal bank regulators should step up enforcement of BSA/AML obligations and scrutinize the institutions into which fraudulent checks are deposited.
- States should amend their UCC laws to remove the ability of banks to shorten the time period provided by the UCC to report altered or forged checks.
- Improvements in the protections for P2P payments would also give consumers more confidence in using those systems instead of checks.

We should also give consideration to moving consumer protections for checks within the EFTA, which provides a clearer framework than the UCC for consumer protection including error resolution timelines and procedures and consumer rights.

The Federal Reserve Banks should also explore collecting information on check fraud, which may help to identify institutions that need to do a better job with their BSA/AML obligations.

VI. Electronic Benefit Transfer (EBT) Card Fraud.

A. EBT card skimming and theft leave cardholders without any protections.

Supplemental Nutrition Assistance Program (SNAP) benefits are distributed and administered through the Electronic Benefit Transfer (EBT) system to eligible participants. EBT has been the sole method of SNAP issuance in all states since June of 2004,[91] and some states also use EBT cards to issue Temporary Assistance for Needy Families (TANF) or other state administered financial assistance.[92] EBT accounts perform the same function for low-income households as do checking accounts— the accounts power daily, or near daily, transactions. People who receive these benefits typically spend down the account balance to $0 each month.

In 2020, about 39.9 million people across the country received SNAP benefits;[93] 38% of whom were white, 25.5% Black, and 15% Hispanic.[94] As of 2022, nearly 2 million Americans receive Temporary Assistance for Needy Families ("TANF") benefits to support their families.[95] In FY

[91] https://www.fns.usda.gov/snap/ebt
[92] https://fns-prod.azureedge.us/sites/default/files/resource-files/ebt-contract-procurement-summary-20221215.pdf
[93] U.S. Department of Agriculture, Food and Nutrition Service "*Characteristics of SNAP Households: FY 2020 and Early Months of the Covid-19 Pandemic: Characteristics of SNAP Households*," available at https://www.fns.usda.gov/snap/characteristics-snap-households-fy-2020-and-early-months-covid-19-pandemic-characteristics.
[94] Cronquist, Kathryn and Eiffes, Brett, "*Characteristics of Supplemental Nutrition Assistance Program Households: Fiscal Year 2020, Table B.4.b. Distribution of participating households by shelter-related characteristics and by State, waiver period*" (Washington: U.S. Department of Agriculture, 2022), available at https://fns-prod.azureedge.us/sites/default/files/resource-files/Characteristics2020.pdf; 7 C.F.R. § 273.10(c)(2)(i).
[95] Office of Family Administration, Administration for Children and Families, "TANF Caseload Data 2022," August 2022, https://www.acf.hhs.gov/ofa/data/tanf-caseload-data-2022.

2021, 35% of TANF recipients were Hispanic, 29% were Black, and 27% were white.[96] These public benefit programs are focused entirely on low-income families.

During the past two years, EBT cardholders have been targeted by criminals who "skim" account information and PINs and then deplete the accounts of all funds belonging to the recipients. This problem is so endemic that even the USDA issued a policy memo on EBT card skimming prevention with tools and resources to prevent and identify the fraud,[97] and Congress recently provided for reimbursement of these stolen funds for the period of October 1, 2022, to September 30, 2024.[98]

However, while other consumers have also been victimized by skimming, EBT consumers are particularly vulnerable and left with little to no recourse. Unlike other cardholders whose funds may be stolen in the same way, EBT cardholders – the lowest-income and most vulnerable consumers – do not have protections afforded to other consumers by the Electronic Funds Transfer Act or Regulation E. Even if the consumer did not lose their card, was not responsible for providing card information to the criminal, and immediately reported missing funds, they are completely out of luck. These lost funds come out of the pockets of the poorest families who cannot afford to lose a single dollar.

B. Potential remedy to address EBT card fraud.

We support legislative efforts to address gaps in the Electronic Fund Transfer Act that leave consumers unprotected. The EFTA and SNAP statute can be amended to address the specific problem of EBT card fraud by eliminating the exclusion of EBT cards from the EFTA and providing protection against unauthorized transfers. As a result, consumers who are impacted by EBT card theft will be able to avail themselves of the EFTA unauthorized use provision and error resolution procedures.

VII. Problems with the collection of accurate payment fraud data create an additional barrier in addressing payment fraud.

A. The problem of fragmented data collection on payment fraud.

In the United States, regulatory oversight and supervision of actors in the payments space depends on several factors including the size, type, and nature of a financial institution,[99] as well

[96] U.S. Department of Health and Human Services, Office of Family Assistance, "*Characteristics and Financial Circumstances of TANF Recipients, Fiscal Year 2021*," updated February 2023, available at https://www.acf.hhs.gov/ofa/data/characteristics-and-financial-circumstances-tanf-recipients-fiscal-year-2021.
[97] https://www.fns.usda.gov/snap/snap-tanf-ebt-card-skimming-prevention
[98] *See* the Consolidated Appropriations Act (CAA) of 2023, Title IV, Section 501.
[99] Depending on the size and activity, a financial institution engaging in payment activity could be subject to supervision by the Office of the Comptroller of the Currency, the Federal Reserve Board, the Federal Deposit Insurance Corporation, the National Credit Union Administration, and/or the Consumer Financial Protection Bureau. Otherwise, the institution could be subject to state regulatory supervision under a state bank charter or money transmitter license. Some payment actors may not be subject to any supervision, though they are still required to comply with all laws.

as the extent to which the activities[100] undertaken by an institution are covered by existing law. As a result, no centralized federal agency receives or collects all data about payment fraud.[101] Additionally, defrauded consumers may report fraud to the Federal Trade Commission, the FBI's internet crimes division, and/or the Consumer Financial Protection Bureau, among other local law enforcement agencies, leading to differing and incomplete snapshots of payment fraud. Although these agencies may share fraud data with each other or the general public, there is no mandate to do so.[102]

Furthermore, financial institutions, payment processors, and payment operators are not required to report the incidents of payment fraud experienced by their customers/consumers to any federal agency. The institutions are required to file a Suspicious Activity Report (SAR) for large transactions in certain circumstances if they suspect their customer is engaged in fraudulent activity, but they are not required to report smaller fraudulent transactions or instances where their clients have been victimized by fraud.[103] Even with SARs mandatory reporting, the information collected by FinCEN relies heavily on the discretion of a financial institution, whether the fraud or potential fraud is discovered/flagged by the reporting institution, and if the transaction is large enough to warrant reporting.[104]

Players in the payment industry have recognized the need for fraud information sharing, and some payment operators do collect data about fraud. The Federal Reserve Board collects reports of fraud on FedNow as specified under Regulation J, Subpart C and keeps a "Negative List" of suspicious accounts that is shared with its participants.[105] The Clearing House also collects fraud reports for RTP® (their real time payments platform) and Early Warning Systems (EWS), owner of Zelle, collects reports of fraud occurring on Zelle, though it is unclear if this information is

---

[100] Though not covered by this testimony, institutions engaged in payments through cryptocurrency and/or stablecoin face the possibility of oversight by the prudential regulators as well as Commodities Futures Trading Commission, the Securities and Exchange Commission, and/or the Consumer Financial Protection Bureau.
[101] Of any type, including fraud through P2P apps, bank-to-bank transfers, or check fraud.
[102] Though certain fraudulent activity is required to be reported to FinCEN, and the Federal Reserve Board will collect fraud data through FedNow. However, FinCEN does not publicly share the data it collects, and it is unclear how the Federal Reserve Board will utilize and disseminate the data it will collect for FedNow.
[103] "Dollar Amount Thresholds- Banks are required to file a SAR in the following circumstances: insider abuse involving any amount; transactions aggregating $5,000 or more where a suspect can be identified; transactions aggregating $25,000 or more regardless of potential suspects; and transactions aggregating $5,000 or more that involve potential money laundering or violations of the BSA. It is recognized, however, that with respect to instances of possible terrorism, identity theft, and computer intrusions, the dollar thresholds for filing may not always be met. Financial institutions are encouraged to file nonetheless in appropriate situations involving these matters, based on the potential harm that such crimes can produce. Even when the dollar thresholds of the regulations are not met, financial institutions have the discretion to file a SAR and are protected by the safe harbor provided for in the statute." From FDIC *"Connecting the Dots… The Important of Timely and Effective Suspicious Activity Reports"* Supervisory Insights (Updated Jul. 10, 2023), available at https://www.fdic.gov/regulations/examinations/supervisory/insights/siwin07/siwinter2007-article03.html#:~:text=Dollar%20Amount%20Thresholds%20%E2%80%93%20Banks%20are,and%20transactions%20aggregating%20%245%2C000%20or.
[104] *See* Mansfield, Cathy, "*It Takes a Thief…. and a Bank: Protecting Consumers From Fraud and Scams on P2P Payment Platforms,"* 57 U. Mich. J.L. Reform (2024).
[105] *See* Operating Circular 8: Funds Transfers through the FedNow Service (Sept. 21, 2022) available at https://www.frbservices.org/binaries/content/assets/crsocms/resources/rules-regulations/operating-circular-8.pdf.

shared widely among users.[106] Even initiatives such as SardineX[107] and Beacon[108] were launched in response to increased fraud in digital payments and real-time payment systems. However, the information shared is not available to the public and may be industry or payment specific. For example, if a bad actor is flagged in one payment system (i.e. Zelle), that does not mean a financial institution will have that bad actor flagged when allowing a fraudulent wire transfer to be released.[109]

The fragmentation described above prevents a clear and cohesive picture of the payment fraud landscape, actors, and trends and poses a barrier to forming effective strategies to combat fraud.

B. Potential remedies to address the problem of fragmented payment fraud data collection.

1. Interagency collaboration.

The importance of information sharing and collaboration between state and federal law enforcement agencies charged with protecting the public from fraud and other unfair, deceptive, and abusive business practices cannot be overstated. Collaboration is essential not only to identify illegal practices that harm consumers, but to facilitate a comprehensive and effective strategy to stop fraudsters before they have stolen money from individuals and families. Criminals know no boundaries; they leverage technology to perpetrate their schemes quickly and are oftentimes unknown until it is too late. Staying ahead of these players requires rigorous and easy lines of communication between partners— including private attorneys and non-profit organizations—who are often the first to hear about scams on the ground.

Indeed, NCLC provided many of the recommendations that follow in comments to the FTC Collaboration Act of 2021.[110] One of these recommendations is that the FTC develop a Fraud Task Force to ensure more regular information sharing and cooperation among all the various agencies that see and deal with individual pieces of the fraud landscape.

---

[106] *See Faster Payments Fraud Trends and Mitigation Opportunities*, Faster Payments Council, Fraud Work Group Bulletin.01 at 5 (Jan 2024), available at https://fasterpaymentscouncil.org/userfiles/2080/files/FPC%20Fraud%20Bulletin_01_01-24-2024_Final.pdf.

[107] *Join sardineX*, Sardine, available at https://go.sardine.ai/sardinex. SardineX is intended as a real-time fraud detection network made up of a consortium of financial institutions and fintech organizations, including banks, card networks, payment processors, and fintechs, which will include a shared database where participants can access fraud data on entities transacting across the network.

[108] Meier, Alain "*Introducing Beacon, the Anti-Fraud Network*," Plaid (June 22, 2023), *available at* https://plaid.com/blog/introducing-plaid-beacon/. Beacon, launched by Plaid, is intended as an anti-fraud network enabling financial institutions and fintech companies to share critical fraud intelligence via API across Plaid. Members contribute by reporting instances of fraud and can use the network to detect if a specific identify has already been associated with fraud.

[109] Any private database of suspected fraud actors could be considered a "consumer reporting agency" (CRA) under the Fair Credit Reporting Act (FCRA). Early Warning Services already acknowledges it is a CRA. See CFPB, List of Consumer Reporting Companies, 2023, at 28, https://files.consumerfinance.gov/f/documents/cfpb_consumer-reporting-companies-list_2023.pdf. As such, these databases would be subject to the file disclosure, accuracy, and dispute resolution rights under the FCRA.

[110] *See* NCLC *et al*., Comments regarding the FTC Collaboration Act of 2021, (Aug. 14, 2023) available at https://www.nclc.org/wp-content/uploads/2023/08/FTC_AG-Fraud-Collaboration-consumer-comments-8-14-23-final3-Lauren-Saunders.pdf.

Since reportfraud.ftc.gov and ic3.gov are two of the most used sites to report fraud, the FTC and the FBI should work with the CFPB, banking regulators, and state Attorneys General (AGs) and local law enforcement to simplify fraud reporting for consumers. Consumers may report fraud to many different places – the local police department, the FBI, an AG, the CFPB, or the FTC. Sometimes police refuse to take fraud reports, viewing fraud as a civil matter. Once a consumer is turned away once place, they may give up. We advise consumers to file a complaint in as many places as possible, but that is cumbersome and not always realistic. Consumers may also find that they are asked for the same information multiple times from different agencies. We urge these agencies to:

- Develop standardized complaint intake forms that can be used by many different agencies.
- Provide a range of easily accessible channels (e.g. in person, phone, e-mail, web, mobile app) for consumers to submit complaints and grievances.
- Include options to report fraud and other complaints in multiple languages.

Fraud reporting must be as simple and universal as possible to be effective.

We also support the provision in Title I of the Senate Appropriation Committee's Financial Services and General Government bill on financial fraud, which directs the Treasury Department to "facilitate a public-private partnership to enhance Americans' financial security and prevent the proliferation of financial fraud and scam schemes… (including) the relevant Federal and State financial regulators, consumer protection agencies, law enforcement, financial institutions, trade associations, consumer and privacy advocates, and other stakeholders."[111] That partnership would "encourage information sharing among participants, develop best practices for relevant stakeholders, including the larger public, develop educational materials to enhance awareness of financial fraud schemes across sectors, share leading practices and tools, and encourage innovations in counter-fraud technologies, data-analytics, and approaches."[112]

2. Require fraud reporting within payment systems.

As previously mentioned, the operators of FedNow, RTP®, and Zelle already collect reports of fraud, and they should analyze those reports, follow up on patterns, and develop preventive measures if they are not already doing so.

But we especially urge the Federal Reserve Board, the operators of other wire transfer services, and other bank regulators to devote attention to bank-to-bank wire transfers. While there is a fair amount of knowledge about how consumers are defrauded into sending funds through wire transfers, no one seems to be collecting or analyzing information about the accounts into which funds are sent. Some of these questions can only be answered by the banks, bank regulators, or wire transfer operators. We understand that the Federal Reserve Board does not receive fraud

[111] Financial Services and General Government Appropriations Bill, 2024. (S. 2309), Title I. Department of the Treasury, "Financial Fraud" at 10, available at https://www.appropriations.senate.gov/imo/media/doc/fy24_fsgg_report.pdf.
[112] *Id.*

reports from institutions utilizing Fedwire, though it may be exploring doing so. We do not know what fraud information is collected on other wire transfer services, such as The Clearing House's CHIPS system.

As previously mentioned, the Federal Reserve Banks should also explore collecting information on check fraud.

The more information law enforcement, payment system operators, and regulators have about fraud committed through these platforms, and the more that agencies work together to identify trends, the more avenues there will be for stopping fraud.

VIII. The use of AI and automated tools to combat payment fraud is important, but consumers need clear rights when innocent consumers are negatively impacted.

A. Overaggressive algorithms can shut out innocent consumers from access to their accounts and funds.

Most parties who engage in payments, (financial institutions, payment processors, card networks, money service businesses, and fintechs) utilize tools to combat payment fraud, including AI and machine learning technologies. Financial institutions who hold consumer deposits may also utilize these same kinds of technologies to comply with their BSA/AML obligations. However, these tools may harm innocent consumers if not utilized properly and if institutions do not have clear procedures and timelines in place to restore access to funds that are improperly frozen.

Sometimes the appropriate response by a company who suspects its customer is engaging in fraudulent activity is to freeze a transaction or close an account that is being used to receive fraudulent funds before the funds are gone and more consumers can be defrauded. However, no law requires the company to take these actions; it is up to the risk tolerance of the company and the internal policies set in place by the company. The only required responses to potential fraud a company may need to undertake under BSA/AML law is to file a Suspicious Activity Report (SAR) if the transaction is large enough to meet the threshold reporting requirements and update their customer risk profile.[113]

According to the Bank Policy Institute, "a sample of the largest banks reviewed approximately 16 million alerts, filed over 640,000 SARs, and received feedback from law enforcement on a median of 4% of those SARs. Ultimately, this means that 90-95% of the individuals that banks report on were likely innocent."[114] As a result, even the filing of a SAR alone should not automatically trigger an account closure.

---

[113] Financial Crimes Enforcement Network, Customer Due Diligence Requirements for Financial Institutions, Final Rule, 81 Fed. Reg. 29398 (May 11, 2016); 31 C.F.R. 1020.210(b)(i); Office of the Comptroller of the Currency, *Bank Secrecy Act (BSA)*, available at https://www.occ.treas.gov/topics/supervision-and-examination/bsa/index-bsa.html/.

[114] Bank Policy Institute "*The Truth About Suspicious Activity Reports*," (Sept. 22, 2020) available at https://bpi.com/the-truth-about-suspicious-activity-reports/ and citing to, "*Getting to Effectiveness—Report on U.S. Financial Institution Resources Devoted to BSA/AML & Sanctions Compliance*," Bank Policy Institute (Oct. 29, 2018) available at https://bpi.com/wp-content/uploads/2018/10/BPI_AML_Sanctions_Study_vF.pdf.

But financial institutions have broad discretion in how they respond to perceived risk threats and have sometimes overreacted to fraud waves, catching innocent consumers in the process. Often, the most vulnerable people have been denied access to their money.

After Chime embarked on a marketing campaign to convince people to open Chime accounts to receive their stimulus payments, its inadequate identity verification led to a wave of fraud. Chime then froze numerous accounts, leaving some people without their money for months on end:

- "Chime stole my entire unemployment backpay…. I'm a single mom of 4 kids and they stolen $1400 from me and refuse to give it back and now we are about to be evicted."[115]

Similarly, Bank of America froze 350,000 unemployment debit cards in California after extensive fraud reports. But the freezes caught many legitimately unemployed workers, and the bank failed to respond in a timely fashion to their complaints:

- "Heather Hauri got a text from Bank of America that suggested her debit card may have been compromised too. When she responded that she had not made the transactions in question, she was locked out of her account. 'The whole account is frozen,' she said. 'You can't get your own money.'"[116]

Months later, after a lawsuit was filed, a judge prohibited the bank from freezing accounts for California unemployment benefits based solely on an automated fraud filter and required it to do a better job of responding when jobless people say their benefits were stolen.[117] The CFPB ultimately brought an enforcement action against Bank of America,[118] and also against U.S. Bank[119] for similar conduct in indiscriminately freezing accounts and leaving them frozen for long periods of time. This conduct harmed the most vulnerable consumers – those who had lost their jobs and were relying on unemployment benefits.

The amount of accountholders who have complained about checking and savings account closures to the CFPB more than doubled since 2017,[120] and in 2022 the CFPB ordered Wells

---

[115] Kessler, Carson, "*A Banking App Has Been Suddenly Closing Accounts, Sometimes Not Returning Customers' Money*," ProPublica (July 6, 2021), available at https://www.propublica.org/article/chime.
[116] KCAL News, "*Bank Of America Freezes EDD Accounts Of Nearly 350,000 Unemployed Californians For Suspected Fraud*," (Oct. 29, 2020), available at https://www.cbsnews.com/losangeles/news/bank-of-america-freezes-edd-accounts-of-nearly-350000-unemployed-californians-for-suspected-fraud/.
[117] McGreevy, Patrick, "*Bank of America must provide more proof of fraud before freezing EDD accounts, court orders,*" Los Angeles Times (Jun. 1, 2021), available at https://www.latimes.com/california/story/2021-06-01/bank-of-america-ordered-to-unfreeze-unemployment-benefit-cards-in-california.
[118] CFPB, "*Federal Regulators Fine Bank of America $225 Million Over Botched Disbursement of State Unemployment Benefits at Height of Pandemic*," (Press Release) (July 14, 2022), available at https://www.consumerfinance.gov/about-us/newsroom/federal-regulators-fine-bank-of-america-225-million-over-botched-disbursement-of-state-unemployment-benefits-at-height-of-pandemic/.
[119] CFPB, "*CFPB Orders U.S. Bank to Pay $21 Million for Illegal Conduct During COVID-19 Pandemic*," (Press Release) (Dec. 19, 2023), available at https://www.consumerfinance.gov/about-us/newsroom/cfpb-orders-us-bank-to-pay-21-million-for-illegal-conduct-during-covid-19-pandemic/#:~:text=The%20CFPB%20and%20OCC%20together,411%2DCFPB%20(2372).
[120] CFPB Consumer Complaint Database trends data for complaints received due to checking or savings account

Fargo to pay $160 million to over one million people for improperly freezing or closing bank accounts from 2011 to 2016 when it "believed that a fraudulent deposit had been made into a consumer deposit account based largely on an automated fraud detection system."[121]

There have been other stories featured by reporters detailing the devastating impact sudden account closures and freezes can have on consumers, especially when they are deprived access to their funds, are not provided with any information about the reason for the institution's actions, and are not provided an opportunity to address any perceived risk.

Following are a few examples from a New York Times article detailing the responses consumers received after discovering their accounts were either frozen or closed and the attempts to communicate with their financial institutions about it: [122]

- Naafeh Dhillon, 28 from Brooklyn, NY, learned his account had been closed after his debit card and credit card were declined. He was later told by a Chase representative that the "bank's global security and investigation team had ultimately made the decision. Would the representative transfer him to that department? Nope… Since he wasn't given a specific reason for the closure, he couldn't disprove whatever raised suspicions in the first place."

- Todd Zolecki, 47 of Media, PA, did not have his account closed, but they did lock him out of access to his account. "They said your account has been suspended for further review," Why? "We can't tell you that. The only thing we can tell you is it can take up to 60 days for this review."

When people cannot access money they need based on red flags triggered by automated fraud tracking systems alone, that problem is compounded when a consumer's complaint is not followed up with any reasonable investigation by the financial institution involving any discussion with the accountholder or any clear timeline to unfreeze their money.

The EFTA has clear error resolution timelines and procedures, and those should be used when consumers cannot access their funds. If a consumer is unable to make an electronic withdrawal or transfer because of an account closure or freeze based on suspected fraud, that action should be viewed as an error – an incorrect transfer of zero instead of the requested amount – triggering the error resolution rights, duties, timelines and investigation procedures of the EFTA. But financial institutions and payment apps seem to believe the EFTA does not apply in this

---

closure available at https://www.consumerfinance.gov/data-research/consumer-complaints/search/?chartType=line&dateInterval=Month&dateRange=All&date_received_max=2024-01-27&date_received_min=2011-12-01&has_narrative=true&issue=Closing%20an%20account%E2%80%A2Company%20closed%20your%20account&lens=Product&product=Checking%20or%20savings%20account&searchField=all&subLens=sub_product&tab=Trends.

[121] *In the Matter of Wells Fargo Bank, N.A.*, CFPB No. 2022-CFPB-0011 (Dec. 20, 2022) (consent order), available at https://files.consumerfinance.gov/f/documents/cfpb_wells-fargo-na-2022_consent-order_2022-12.pdf.

[122] Barnard, Tara Siegel and Lieber, Ron, "*Banks Are Closing Customer Accounts, With Little Explanation*," New York Times (Apr. 8, 2023) available at https://www.nytimes.com/2023/04/08/your-money/bank-account-suspicious-activity.html?unlocked_article_code=1.QU0.szRm.kfoZRQdD7-O6&smid=url-share.

situation.

B. Potential remedies to address improper freezes or account closures due to the use of automated fraud detection.

We support legislative efforts to address the many gaps and ambiguities in the Electronic Fund Transfer Act that leave consumers unprotected. The EFTA can be amended to address the specific problem of improper freezes and account closures by clarifying that the error resolution duties under the EFTA apply if a consumer's account is frozen or closed or the consumer is otherwise unable to access their funds. When a consumer contacts their financial institution complaining about the inability to access funds or an account closure, the institution would have to perform a reasonable investigation and provide a resolution to the consumer within 10 days or provide a provisional, unfrozen, credit pending a longer investigation. After a reasonable investigation, the consumer's financial institution would have to release the frozen funds or reopen a closed account if it was done in error—except in cases where the consumer obtained the funds through unlawful or fraudulent means or was denied access due to a court order or as directed by law enforcement.

The EFTA's error resolution procedures allow financial institutions to continue using automated fraud detection systems while ensuring that consumers have remedies when those systems get it wrong. This would ensure a consumer receives information about why their account was frozen or closed and get more timely access to their funds if the bank was in error.

The problem with account closures and freezes could also be addressed by rulemaking or guidance from the CFPB.

FinCEN and bank regulators should also provide guidance to financial institutions about what information they may and should provide to accountholders regarding freezes and account closures while still complying with the BSA. For example, they could clarify in a FAQ that, while financial institutions are not allowed to disclose that a SAR was filed, they are allowed to disclose that an account was frozen or closed due to suspicious activity and/or describe the specific activities that raised concerns.

As shown by the CFPB's recent enforcement actions and in light of risks of unfair, deceptive, or abusive practices when consumers' funds are held indefinitely, the CFPB and bank regulators should also provide guidance to financial institutions about the importance of having clear procedures to enable consumers to quickly regain access to their funds when they are frozen due to concerns of suspicious activity and provide guidance as to the timeliness of returning an accountholder's funds after account closure.

IX. Conclusion

Payment fraud is a pervasive problem impacting U.S. consumers, especially those most vulnerable to the loss of income caused by unauthorized and fraudulently induced transactions. However, Congress can take steps to address these problems by utilizing a holistic approach to the problems caused by fraud and scams instead of just relying on consumer education and information dissemination.

With any questions, please contact Carla Sanchez-Adams, Senior Attorney at the National Consumer Law Center, at csanchezadams@nclc.org.

Thank you for the opportunity to provide this statement for the record.

Yours very truly,

National Consumer Law Center (on behalf of its low-income clients)

Purchase and Sale of Future Receipts Agreement

Seller's Legal Name Hiteks Solutions, Inc.	D/B/A Hiteks	Form of Business Entity Corporation	State of Incorporation New York
Street Address 447 Broadway Floor 2	City, State New York, New York	Zip 10013	
Mailing Address 1356 Union Club Drive	City, State Winter Garden, Florida	Zip 34787	
Primary Contact Name Gerasimos Petratos	Primary Contact Title Owner	Seller's Tax ID: [redacted]7472	
Seller's Bank Account Citibank	ABA Transit/Routing #: [redacted]0089	Checking Account #: [redacted]8065	
Purchase Price $199,000.00	Purchased Amount of Future Receipts $258,700.00	Specified Percentage 11.51%	
Origination Fee (Deducted from Purchase Price): $5,970.00			
Remittance Frequency *Weekly Every* ***Thursday***		Initial Remittance Amount: $6,843.92	
How we determine the Remittance Amount: We review information you provide or make available to us to calculate your total sales revenue over a period of time prior to the date of this Agreement. We then estimate the average amount of your sales revenue per the Remittance Frequency described above. Then we multiply this amount by the Specified Percentage above and this is your initial Remittance Amount. Please refer to Section 4 of this Agreement for how the Remittance Amount can be changed.			
Net Amount Funded to Seller (This is the Purchase Price less the Origination Fee): **$193,030.00**			

This Purchase and Sale of Future Receipts Agreement ("Agreement") effective, 22 February, 2024 is made by and between Legend Advance Funding II, LLC located at 800 Brickell Avenue, Suite 902, Miami, Florida 33131 ("Buyer") [making Buyer on behalf of itself and its co-investors the absolute owner], the business identified above ("Seller"), and each Guarantor identified below (each a "Guarantor").

Seller, hereby sells and assigns to Buyer, without recourse, the Purchased Amount and will deliver the Specified Percentage of the proceeds of each future sale made by Seller (collectively "Future Receipts") in accordance with this Agreement.

Agreement of Seller: By signing below Seller agrees to the terms and conditions contained in this Agreement, including those terms and conditions on the following pages, and further agrees that this transaction is for business purposes and not for personal, family, or household purposes.

Seller Hiteks Solutions, Inc.		
Agreed to by Gerasimos Petratos	Signature	Title Owner
Agreed to by N/A	Signature	Title N/A

Initial Here

Agreed to by N/A	Signature	Title N/A
Agreed to by N/A	Signature	Title N/A

Agreement of Each Guarantor: By signing below each Guarantor agrees to the terms and conditions contained in this Agreement, including those terms and conditions on the following pages, and further agrees that this transaction is for business purposes and not for personal, family, or household purposes.

Notice: This agreement contains a personal guaranty of performance, and by signing below, you agree that you will be personally liable for the prompt and complete performance of obligations of the Seller as described in this Agreement.

Agreed to by Gerasimos Petratos	Address 1356 Union Club Drive, Winter Garden, Florida, 34787	Signature
Agreed to by N/A	Address N/A, N/A,	Signature
Agreed to by N/A	Address N/A, N/A, N/A	Signature
Agreed to by N/A	Address N/A, N/A, N/A	Signature

Terms and Conditions

1. **Future Receipts.** "Future Receipts" includes all payments made by cash, check, Automated Clearing House ("ACH") or other electronic transfer, credit card, debit card, bank card, charge card (each such card shall be referred to herein as a "Payment Card") or other form of monetary payment in the ordinary course of Seller's business. As payment for the Purchased Amount, Buyer will pay to Seller the Purchase Price, minus any amounts shown above.

2. **Buyer's Acceptance of Agreement.** The obligation of Buyer under this Agreement will not be effective unless and until Buyer has completed its review of the Seller and has accepted this Agreement by delivering the Net Amount Funded to Seller, shown above. Prior to accepting this Agreement, Buyer may conduct a processing trial to confirm its access to Seller's Bank Account, shown above (the "Account") and the ability to withdraw the Remittance Amount. If the processing trial is not completed to the satisfaction of Buyer, Buyer will refund to Seller all funds that were obtained by Buyer during the processing trial.

3. **Delivery of Purchased Amount.**

   a. **Seller to Deposit Future Receipts Each Day.** Seller must deposit all Future Receipts into the Account on a daily basis and must instruct Seller's credit card processor, which must be approved by Buyer (the "Processor") to deposit all Payment Card receipts of Seller into the Account on a daily basis. Seller agrees not to change the Account or add an additional Account without the express written consent of Buyer.

   b. **Authorization for Buyer to Debit Remittance Amount.** Seller authorizes Buyer to debit the Remittance Amount from the Account according to the Remittance Frequency by either ACH or electronic check. Seller will provide Buyer with all required account information necessary to initiate such checks or debit entries. Seller will provide an appropriate ACH authorization to Buyer. If any draft or electronic debit is returned for insufficient funds, then Seller will be responsible for any fees incurred by Buyer resulting from a rejected electronic check or ACH debit attempt, as set forth on Appendix A. If the Remittance Frequency is weekly, Buyer may change the Remittance Frequency to daily if Seller's weekly remittance is rejected for any reason during the course of this Agreement. Buyer is not responsible for any overdrafts or rejected transactions that may result from Buyer's debiting any amount authorized under the terms of this Agreement. Seller understands that the foregoing ACH authorization is a fundamental condition to induce Buyer to

accept the Agreement. Consequently, such authorization is intended to be irrevocable. In the event that Seller changes or permits changes to the Account or the ACH authorization approved by the Buyer or adds an additional bank account, Buyer shall have the right, without waiving any of its rights and remedies and without notice to Seller or any Guarantor, to notify the new or additional bank of this Agreement and to direct such new or additional bank to remit to the Buyer all or any portion of the amounts received by such bank.

4. **Changes to the Remittance Amount (IMPORTANT PROTECTION FOR SELLER).** The initial Remittance Amount is intended to represent the Specified Percentage of Seller's periodic Future Receipts. At any time during the course of this Agreement, Seller or Buyer may request an adjustment to the Remittance Amount to more closely reflect the Seller's actual Future Receipts times the Specified Percentage. Seller agrees to provide Buyer requested bank statements or other records of Seller's actual revenue to assist in this reconciliation. Within five days of Buyer's reasonable verification of such information, Buyer shall adjust the Remittance Amount on a going-forward basis to more closely reflect the Seller's actual Future Receipts times the Specified Percentage. Buyer will notify Seller prior to any such adjustment. After each adjustment made pursuant to this paragraph, the new dollar amount shall be deemed the Remittance Amount until any subsequent adjustment. To request an adjustment to the Remittance Amount call 888-851-8859 or email customersupport@legendfunding.com.

5. **Remittance Amount Upon Default.** Upon the occurrence of an Event of Default, the Remittance Amount shall equal 100% of all Future Receipts.

6. **Nonrecourse Sale of Future Receipts (THIS IS NOT A LOAN).** Seller is selling a portion of a future revenue stream to Buyer at a discount, not borrowing money from Buyer. There is no interest rate or payment schedule and no time period during which the Purchased Amount must be collected by Buyer. Seller acknowledges that it has no right to repurchase the Purchased Amount from Buyer. Buyer assumes the risk that Future Receipts may be remitted more slowly than Buyer may have anticipated or projected because Seller's business has slowed down, and the risk that the full Purchased Amount may never be remitted because Seller's business went bankrupt or Seller otherwise ceased operations in the ordinary course of business. Buyer is buying the Purchased Amount of Future Receipts knowing the risks that Seller's business may slow down or fail, and Buyer assumes these risks based on Seller's representations, warranties and covenants in this Agreement that are designed to give Buyer a reasonable and fair opportunity to receive the benefit of its bargain. By this Agreement, Seller transfers to Buyer full and complete ownership of the Purchased Amount of Future Receipts and Seller retains no legal or equitable interest therein. Seller agrees that it will treat the Purchase Price and Purchased Amount in a manner consistent with a sale in its accounting records and tax returns. Seller agrees that Buyer is entitled to audit Seller's accounting records upon reasonable Notice in order to verify compliance. Seller waives any rights of privacy, confidentiality or taxpayer privilege in any such litigation or arbitration in which Seller asserts that this transaction is anything other than a sale of future receipts.

7. **Fees and Charges.** Other than the Origination Fee, if any, set forth above, Buyer is NOT CHARGING ANY ORIGINATION OR BROKER FEES to Seller. If Seller is charged another such fee, it is not being charged by Buyer. A list of all fees and charges applicable under this Agreement is contained in Appendix A.

8. **Credit Report and Other Authorizations.** Seller and each of the Owners signing above authorize Buyer, its agents and representatives and any credit reporting agency engaged by Buyer, to (i) investigate any references given or any other statements or data obtained from or about Seller or any of its Owners for the purpose of this Agreement; (ii) obtain consumer and business credit reports on the Seller and any of its Owners; and (iii) to contact personal and business references provided by the Seller in the Application, at any time now or for so long as Seller and/or Owners continue to have any obligations to Buyer as a consequence of this Agreement or for Buyer's ability to determine Seller's eligibility to enter into any future agreement with Buyer.

9. **Authorization to Contact Current and Prior Banks.** Seller hereby authorizes Buyer to contact any current or prior bank of the Seller in order to obtain whatever information it may require regarding Seller's transactions with any such bank. Such information may include but is not limited to, information necessary to verify the amount of Future Receipts previously processed on behalf of Seller and any fees that may have been charged by the bank. In addition, Seller authorizes Buyer to contact any current or prior bank of the Seller for collections and in order to confirm that Seller is exclusively using the Account identified above, or any other account approved by Buyer, for the deposit of all business receipts.

Initial Here

10. **Right to Cancel.** Seller understands that Buyer offers Seller a right to cancel this Agreement at any time within 3 days after Buyer has delivered the Net Amount Funded. Seller may exercise this right by notifying Buyer that it is cancelling this Agreement and returning to Buyer all amounts Buyer has paid to Seller or paid to third parties on behalf of Seller. For the Seller's right to cancel to be effective, Buyer must receive both the notice and the return of the funds within 3 days after the Buyer has delivered the Net Amount Funded.

11. **Financial Information.** Seller authorizes Buyer and its agents to investigate its financial responsibility and history, and will provide to Buyer any authorizations, bank or financial statements, tax returns, etc., as Buyer deems necessary in its sole discretion prior to or at any time after execution of this Agreement. A photocopy of this authorization will be deemed acceptable as an authorization for release of financial and credit information. Buyer is authorized to update such information and financial and credit profiles from time to time as it deems appropriate. Seller waives, to the maximum extent permitted by law, any claim for damages against Buyer or any of its affiliates relating to any investigation undertaken by or on behalf of Buyer as permitted by this Agreement or disclosure of information as permitted by this Agreement.

12. **Transactional History.** Seller authorizes all of its banks and brokers and Payment Card processors to provide Buyer with Seller's banking, brokerage and/or processing history to determine qualification or continuation in this program, or for collections upon an Event of Default.

13. **Publicity.** Seller hereby authorizes Buyer to use its name in listings of clients and in advertising and marketing materials.

14. **Application of Amounts Received by Buyer.** Buyer reserves the right to apply amounts received by it under this Agreement to any fees or other charges due to Buyer from Seller prior to applying such amounts to reduce the amount of any outstanding Purchased Amount.

15. **Representations, Warranties and Covenants of Seller.** As of the date of this Agreement and, unless expressly stated otherwise, continuing until Buyer has received 1) the Purchased Amount and 2) all fees and charges (including legal fees) due under this Agreement, Seller represents, warrants and covenants to Buyer as follows:

    a. **No Diversion of Future Receipts.** Seller must deposit all Future Receipts into the Account on a daily basis and must instruct the Processor to deposit all Payment Card receipts of Seller into an authorized Account on a daily basis. Seller agrees not to (i) change the Account without the express written consent of Buyer, (ii) create any new depository account, (iii) revoke Buyer's authorization to debit the Account, (iv) close the Account without the express written consent of Buyer or, (v) take any other action that denies, or interferes with, Buyer's rights under this Agreement, including but not limited to Buyer's right to receive its share of revenue received by Seller.

    b. **Stacking Prohibited.** Seller shall not enter into any financing agreement or any loan agreement on or after the date of this Agreement that relates to or encumbers its Future Receipts or requires daily payments with any party other than Buyer for the duration of this Agreement. Buyer may share information regarding this Agreement with any third party in order to determine whether Seller is in compliance with this provision.

    c. **Financial Condition and Financial Information.** Any bank statements and financial statements of Seller that have been furnished to Buyer, and future statements that will be furnished to Buyer, fairly represent the financial condition of Seller at such dates, or any change in the ownership of Seller. Buyer may request bank statements and copies of and/or electronic access to reasonable documentation of Merchant's card processing activity or financial, banking, or tax affairs at any time during the performance of this Agreement, and Seller shall provide them to Buyer within five business days of such request. Furthermore, Seller represents that all documents, forms and recorded interviews provided to or with Buyer are true, accurate and complete in all respects, and accurately reflect Seller's financial condition and results of operations at the time they are provided. Seller further agrees to authorize the release of any past or future tax returns to Buyer.

    d. **Governmental Approvals.** Seller is in compliance and shall comply with all laws and has valid permits, authorizations and licenses to own, operate and lease its properties and to conduct the business in which it is presently engaged and/or will engage in hereafter.

Initial Here

e. **Authority to Enter Into This Agreement.** Seller and the person(s) signing this Agreement on behalf of Seller, have full power and authority to incur and perform the obligations under this Agreement, all of which have been duly authorized.

f. **Change of Name or Location or Sale or Closing of Business.** Seller will not conduct Seller's businesses under any name other than as disclosed to Buyer or change any of its places of business without prior written consent of Buyer. Seller will not voluntarily sell, dispose, transfer or otherwise convey all or substantially all of its business or assets without (i) the express prior written consent of Buyer; and (ii) the written agreement of any purchaser or transferee assuming all of Seller's obligations under this Agreement pursuant to documentation satisfactory to Buyer. Except as disclosed to Buyer in writing, Seller has no current plans to close its business either temporarily, whether for renovations, repairs or any other purpose, or permanently. Seller will not voluntarily close its business on a temporary basis for renovations, repairs, or any other purposes. This provision, however, does not prohibit Seller from closing its business temporarily if such closing is required to conduct renovations or repairs that are required by local ordinance or other legal order, such as from a health or fire inspector, or if otherwise forced to do so by circumstances outside of the control of Seller. Prior to any such closure, Seller will provide Buyer ten business days' notice to the extent practicable.

g. **No Pending or Contemplated Bankruptcy as of the Date of this Agreement.** As of the date of this Agreement, Seller does not contemplate and has not filed any petition for bankruptcy protection under Title 11 of the United States Code and there has been no involuntary petition brought or pending against Seller. Seller represents that it has not consulted with a bankruptcy attorney within six months prior to the date of this Agreement. Seller further warrants that as of the date of this Agreement it does not anticipate filing a bankruptcy petition and it does not anticipate that an involuntary petition will be filed against it.

h. **Seller to Pay Taxes Promptly.** Seller will promptly pay all necessary taxes, including but not limited to employment and sales and use taxes.

i. **No Violation of Prior Agreements.** Seller's execution and performance of this Agreement will not conflict with any other agreement, obligation, promise, court order, administrative order or decree, law or regulation to which Seller is subject, including any agreement that prohibits the sale or pledge of Seller's Future Receipts.

j. **No Diversion of Receipts.** Seller will not permit any event to occur that could cause a diversion of any of Seller's Future Receipts from the Account.

k. **Seller's Knowledge and Representation.** Seller represents, warrants, and agrees that it is a sophisticated business entity familiar with the kind of transaction covered by the Agreement; it was represented by counsel or had full opportunity to consult with counsel.

l. **Accurate and Complete Information.** Seller represents, warrants, and agrees that all information provided to Buyer, all statements made to Buyer relating to this transaction in any way have been truthful, accurate, and complete. Seller further agrees that Seller will be truthful in all future statements to Buyer, and will provide Buyer with accurate and complete information regarding Seller's business as required by this Agreement.

16. Rights of Buyer.

a. **Acknowledgment of Security Interest and Security Agreement.** The Future Receipts sold by Seller to Buyer pursuant to this Agreement shall constitute and shall be construed and treated for all purposes as a true and complete sale, conveying good title to the Future Receipts free and clear of any undisclosed liens and encumbrances, from Seller to Buyer. To the extent the Future Receipts are "accounts" or "payment intangibles" as those terms are defined in the Uniform Commercial Code as in effect in the state in which the Seller is located ("UCC") then: (i) the sale of the Future Receipts creates a security interest as defined in the UCC; (ii) this Agreement constitutes a "security agreement" under the UCC; and (iii) Buyer has all the rights of a secured party under the UCC with respect to such Future Receipts. Seller further agrees that, with or without an Event of Default, Buyer may notify account debtors, or other persons obligated on the

Initial Here

Future Receipts, or holding the Future Receipts, of Seller's sale of the Future Receipts and may instruct them to make payment or otherwise render performance to or for the benefit of Buyer.

b. **Financing Statements.** Seller authorizes Buyer to file one or more UCC-1 forms consistent with the UCC to give notice that the Purchased Amount of Future Receipts is the sole property of Buyer. The UCC filing may state that such sale is intended to be a sale and not an assignment for security and may state that the Seller is prohibited from obtaining any financing that impairs the value of the Future Receipts or Buyer's right to collect same. Seller authorizes Buyer to debit the Account for all costs incurred by Buyer associated with the filing, amendment or termination of any UCC filings.

c. **Right of Access.** In order to ensure that Seller is complying with the terms of this Agreement, Buyer shall have the right to (i) enter, without notice, the premises of Seller's business during regular business hours for the purpose of inspecting and checking Seller's transaction processing terminals to ensure the terminals are properly programmed to submit and or batch Seller's daily receipts to the Processor and to ensure that Seller has not violated any other provision of this Agreement; (ii) Seller shall provide access to its employees and records and all other items as reasonably requested by Buyer; and (iii) have Seller provide information about its business operations, banking relationships, vendors, landlord and other information to allow Buyer to interview any relevant parties.

d. **Phone Recordings and Contact.** Seller agrees that any call between Buyer and Seller, and their agents and employees may be recorded or monitored. Further, Seller agrees that (i) it has an established business relationship with Buyer, its employees and agents and that Seller may be contacted from time-to-time regarding this or other business transactions; (ii) that such communications and contacts are not unsolicited or inconvenient; and (iii) that any such contact may be made at any phone number, email address, or facsimile number given to Buyer by the Seller, its agents or employees, including cellular telephones.

e. **ACH Authorization.** Seller represents and warrants that (i) the Account is Seller's bank account; (ii) the person executing this Authorization on behalf of Seller is an authorized signer on the Account and has the power and authority to authorize Buyer to initiate ACH transactions to and from the Account; and (iii) the Account is a legitimate, open, and active bank account used solely for business purposes and not for personal, family or household purposes. If an ACH transaction is rejected by Seller's financial institution for any reason other than a stop payment order placed by Seller with its financial institution, including without limitation insufficient funds, Seller agrees that Buyer may resubmit up to two times any ACH transaction that is dishonored. Seller's bank may charge Seller fees for unsuccessful ACH entries. Seller agrees that Buyer will have no liability to Seller for such fees. In the event Buyer makes an error in processing any payment or credit, Seller authorizes Buyer to initiate ACH entries to or from the Account to correct the error. Seller acknowledges that the origination of ACH entries to and from the Account must comply with applicable law and applicable network rules. Seller agrees to be bound by the Rules and Operating Guidelines of NACHA (formerly known as the National Automated Clearing House Association). Seller will not dispute any ACH transaction initiated pursuant to this Authorization, provided the transaction corresponds to the terms of this Authorization. Seller requests the financial institution that holds the Account to honor all ACH entries initiated in accordance with this Authorization.

17. Events of Default. The occurrence of any of the following events shall constitute an "Event of Default": (a) Seller intentionally interferes with Buyer's right to collect the Remittance Amount; (b) Seller violates any term or covenant in this Agreement; (c) Seller uses multiple depository accounts without the prior written consent of Buyer; (d) Seller revokes the ACH Authorization; (e) Seller changes its depositing account or its payment card processor without the prior written consent of Buyer; or (f) Seller defaults under any other agreement with Buyer, or breaches any of the terms, covenants and conditions of any other agreement with Buyer.

18. Remedies. If any Event of Default occurs, Buyer may proceed to protect and enforce its rights including, but not limited to, the following:

a. The Specified Percentage shall equal 100%. The full undelivered Purchased Amount plus all fees and charges (including legal fees) assessed under this Agreement will become due and payable in full immediately.

Initial Here

b. Buyer may charge a Default Fee of the lesser of $5,000 or 25% of amount of undelivered Purchased Amount at the time of the Event of Default.

c. Buyer may enforce the provisions of the Personal Guaranty of Performance against each Owner.

d. Seller shall pay to Buyer all reasonable costs associated with the Event of Default. Buyer may proceed to protect and enforce its rights and remedies by arbitration or lawsuit. In any such arbitration or lawsuit, under which Buyer shall recover Judgment against Seller, Seller shall be liable for all of Buyer's costs, including but not limited to all reasonable attorneys' fees and court costs. However, the rights of Buyer under this provision shall be limited as provided in the arbitration provision set forth below.

e. Buyer may debit Seller's depository accounts wherever situated by means of ACH debit or facsimile signature on a computer-generated check drawn on any of Seller's bank accounts for all sums due to Buyer.

f. Subject to arbitration as provided in Section 33 of this Agreement, all rights, powers and remedies of Buyer in connection with this Agreement may be exercised at any time by Buyer after the occurrence of an Event of Default, are cumulative and not exclusive, and shall be in addition to any other rights, powers or remedies provided by law or equity.

19. Modifications; Amendments. No modification, amendment, waiver or consent of any provision of this Agreement shall be effective unless the same is in writing and signed by Buyer.

20. Assignment. Buyer may assign, transfer or sell its rights to receive the Purchased Amount or delegate its duties hereunder, either in whole or in part, with or without prior written notice to Seller.

21. Personal Guaranty of Performance. Guarantor agrees to irrevocably, absolutely and unconditionally guarantee to Buyer prompt and complete performance of the following obligations of Seller (the "Guaranteed Obligations"):

a. Seller's obligation to deposit all Future Receipts into the Account on a daily basis and instruct the Processor to deposit all Payment Card receipts of Seller into an authorized Account on a daily basis;

b. Seller's obligation to not (i) change the Account without the express written consent of Buyer, (ii) create any new depository account, (iii) revoke Buyer's authorization to debit the Account, (iv) close the Account without the express written consent of Buyer or, (v) take any other action that denies, or interferes with, Buyer's rights under this Agreement, including but not limited to Buyer's right to receive its share of revenue received by Seller;

c. Seller's obligation to provide bank statements and copies of and/or electronic access to reasonable documentation of Merchant's card processing activity or financial, banking or tax affairs within five business days after request from Buyer;

d. Seller's obligation to not change its payment card processor, change its bank account, or add bank accounts;

e. Seller's obligation to not conduct Seller's businesses under any name other than as disclosed to Buyer;

f. Seller's obligation to not change any of its places of business without prior written consent by Buyer;

g. Seller's obligation to not voluntarily sell, dispose, transfer or otherwise convey its business or substantially all business assets without (i) the express prior written consent of Buyer, and (ii) the written agreement of any purchaser or transferee assuming all of Seller's obligations under this Agreement pursuant to documentation satisfactory to Buyer;

h. Seller's obligation to not enter into any financing transaction or any loan agreement that relates to or encumbers its Future Receipts with any party other than Buyer for the duration of this Agreement without Buyer's prior written consent; and

Initial Here

i. Seller's obligation to provide truthful, accurate, complete, and timely information as required by this Agreement.

22. **Guarantor Waivers.** Buyer does not have to notify Guarantor of any of the following events and Guarantor will not be released from its obligations under the Agreement and this Personal Guaranty of Performance if it is not notified of: (i) Seller's failure to timely perform any obligation under the Agreement; (ii) any adverse change in Seller 's financial condition or business; (iii) Buyer's acceptance of the Agreement; and (iv) any renewal, extension or other modification of the Agreement or Seller 's other obligations to Buyer. In addition, Buyer may take any of the following actions without releasing Guarantor from any of its obligations under the Agreement and this Performance Guaranty: (i) renew, extend or otherwise modify the Agreement or Seller's other obligations to Buyer; and (ii) release Seller from its obligations to Buyer. Guarantor shall not seek reimbursement from Seller or any other guarantor for any amounts paid by it under the Agreement or this Performance Guaranty. Guarantor permanently waives and shall not seek to exercise any of the following rights that it may have against Seller, or any other guarantor, for any amounts paid by it, or acts performed by it, under the Agreement or this Performance Guaranty: (i) subrogation; (ii) reimbursement; (iii) performance; (iv) indemnification; or (v) contribution.

23. **Guarantor Acknowledgement**. Guarantor acknowledges that Guarantor understands the seriousness of the provisions of the Agreement, including the Jury Waiver, Class Action Waiver and Arbitration sections, and has had a full opportunity to consult with counsel their choice; and have consulted with counsel or have decided not to avail himself / herself / themselves of that opportunity.

24. **Notices.**

a. **Notices from Buyer.** Buyer may send any notices, disclosures, terms and conditions, other documents, and any future changes to Seller by regular mail or by e-mail, at Buyer's option and Seller consents to such electronic delivery. Notices sent by e-mail are effective when sent. Notices sent by regular mail become effective three days after mailing to Seller's address set forth in this Agreement.

b. **Notices from Seller and Guarantor.** Seller and Guarantor may send any notices to Buyer by e-mail only upon the prior written consent of Buyer, which consent may be withheld or revoked at any time in Buyer's sole discretion. Otherwise, any notices or other communications from Seller and Guarantor to Buyer must be delivered by certified mail, return receipt requested, to Buyer's address set forth in this Agreement. Notices sent to Buyer shall become effective only upon receipt by Buyer.

25. **Binding Effect; Governing Law, Venue and Jurisdiction.** This Agreement shall be binding upon and inure to the benefit of Seller, Buyer and their respective successors and assigns, except that Seller shall not have the right to assign its rights hereunder or any interest herein without the prior written consent of Buyer which consent may be withheld in Buyer's sole discretion. Except as set forth in the Arbitration section, this Agreement shall be governed by and construed in accordance with the laws of the state of Florida, without regard to any applicable principles of conflicts of law. Seller and Guarantor understand and agree that (i) Buyer is located in Florida; (ii) Buyer makes all decisions from Buyer's office in Florida; (iii) the Agreement is made in Florida (that is, no binding contract will be formed until Buyer receives and accepts Seller's signed Agreement in Florida); and (iv) Seller's payments are not accepted until received by Buyer in Florida. Any suit, action or proceeding arising hereunder, or the interpretation, performance or breach of this Agreement, shall, if Buyer so elects, be instituted in any court sitting in Florida, (the "Acceptable Forums"). Seller and Guarantor agree that the Acceptable Forums are convenient to it, and submit to the jurisdiction of the Acceptable Forums and waives any and all objections to jurisdiction or venue. Should such proceeding be initiated in any other forum, Seller and Guarantor waive any right to oppose any motion or application made by Buyer to transfer such proceeding to an Acceptable Forum. Buyer, Seller and Guarantor further agree that the mailing by certified or registered mail, return receipt requested, of any process required by any such court will constitute valid and lawful service of process against them, without the necessity for service by any other means provided by statute or rule of court, but without invalidating service performed in accordance with such other provisions.

26. **Survival of Representations, Warranties and Covenants.** All representations, warranties and covenants herein shall survive the execution and delivery of this Agreement and shall continue in full force until all obligations under this Agreement shall have been satisfied in full.

27. **Interpretation.** All Parties hereto have had the opportunity to review this Agreement with an attorney of their own choosing and have relied only on their own attorney's guidance and advice or have been provided sufficient opportunity to have an attorney of their choosing review the Agreement. No construction determinations shall be made against either Party hereto as drafter.

28. **Entire Agreement and Severability.** This Agreement embodies the entire agreement between Seller and Buyer and supersedes all prior agreements and understandings relating to the subject matter hereof. In case any of the provisions in this Agreement is found to be invalid, illegal or unenforceable in any respect, the validity, legality and enforceability of any other provision contained herein shall not in any way be affected or impaired.

29. **Facsimile Acceptance.** Facsimile signatures, or any other electronic means reflecting the party's signature hereto, shall be deemed acceptable for all purposes. This Agreement may be signed in one or more counterparts, each of which shall constitute an original and all of which when taken together shall constitute one and the same agreement.

30. **Monitoring, Recording, and Solicitations.**

    a. **Authorization to Contact Seller by Phone.** Seller and Guarantor authorize Buyer, its affiliates, agents and independent contractors to contact Seller or Guarantor at any telephone number Seller or Guarantor provide to Buyer or from which Seller or Guarantor places a call to Buyer, or any telephone number where Buyer believes it may reach Seller or Guarantor, using any means of communication, including but not limited to calls or text messages to mobile, cellular, wireless or similar devices or calls or text messages using an automated telephone dialing system and/or artificial voices or prerecorded messages, even if Seller or Guarantor incurs charges for receiving such communications.

    b. **Authorization to Contact Seller by Other Means.** Seller and Guarantor also agree that Buyer, its affiliates, agents and independent contractors, may use any other medium not prohibited by law including, but not limited to, mail, e-mail and facsimile, to contact Seller and Guarantor. Seller and Guarantor expressly consent to conduct business by electronic means.

31. **JURY WAIVER. THE PARTIES WAIVE THE RIGHT TO A TRIAL BY JURY IN ANY COURT IN ANY SUIT, ACTION OR PROCEEDING ON ANY MATTER ARISING IN CONNECTION WITH OR IN ANY WAY RELATED TO THE TRANSACTIONS OF WHICH THIS AGREEMENT IS A PART OR ITS ENFORCEMENT, EXCEPT WHERE SUCH WAIVER IS PROHIBITED BY LAW OR DEEMED BY A COURT OF LAW TO BE AGAINST PUBLIC POLICY. THE PARTIES ACKNOWLEDGE THAT EACH PARTY MAKES THIS WAIVER KNOWINGLY, WILLINGLY AND VOLUNTARILY AND WITHOUT DURESS, AND ACKNOWEDGE THEIR RIGHT TO REVIEW THE RAMIFICATIONS OF THIS WAIVER WITH THEIR ATTORNEYS.**

32. **CLASS ACTION WAIVER. BUYER, SELLER, AND EACH GUARANTOR ACKNOWLEDGE AND AGREE THAT THE AMOUNT AT ISSUE IN THIS TRANSACTION AND ANY DISPUTES THAT ARISE BETWEEN THEM ARE LARGE ENOUGH TO JUSTIFY DISPUTE RESOLUTION ON AN INDIVIDUAL BASIS. EACH PARTY HERETO WAIVES ANY RIGHT TO ASSERT ANY CLAIMS AGAINST THE OTHER PARTIES AS A REPRESENTATIVE OR MEMBER IN ANY CLASS OR REPRESENTATIVE ACTION, EXCEPT WHERE SUCH WAIVER IS PROHIBITED BY LAW OR DEEMED BY A COURT OF LAW TO BE AGAINST PUBLIC POLICY. TO THE EXTENT ANY PARTY IS PERMITTED BY LAW OR A COURT OF LAW TO PROCEED WITH A CLASS OR REPRESENTATIVE ACTION AGAINST THE OTHER, THE PARTIES AGREE THAT: (I) THE PREVAILING PARTY SHALL NOT BE ENTITLED TO RECOVER ATTORNEYS' FEES OR COSTS ASSOCIATED WITH PURSUING THE CLASS OR REPRESENTATIVE ACTION (NOT WITHSTANDING ANY OTHER PROVISION IN THIS AGREEMENT); AND (II) THE PARTY WHO INITIATES OR PARTICIPATES AS A MEMBER OF THE CLASS WILL NOT SUBMIT A CLAIM OR OTHERWISE PARTICIPATE IN ANY RECOVERY SECURED THROUGH THE CLASS OR REPRESENTATIVE ACTION.**

33. **ARBITRATION. IF BUYER, SELLER OR ANY GUARANTOR REQUESTS, THE OTHER PARTIES AGREE TO ARBITRATE ALL DISPUTES AND CLAIMS ARISING OUT OF OR RELATING TO THIS AGREEMENT. IF BUYER, SELLER OR ANY GUARANTOR SEEKS TO HAVE A DISPUTE SETTLED BY ARBITRATION, THAT PARTY MUST FIRST SEND TO ALL OTHER PARTIES, BY CERTIFIED MAIL, A WRITTEN NOTICE OF INTENT TO ARBITRATE. IF BUYER, SELLER OR ANY GUARANTOR DO NOT REACH AN AGREEMENT TO RESOLVE THE CLAIM WITHIN 30 DAYS AFTER THE NOTICE IS RECEIVED, BUYER, SELLER OR ANY GUARANTOR MAY COMMENCE AN ARBITRATION PROCEEDING WITH THE AMERICAN ARBITRATION ASSOCIATION ("AAA") OR THE FORUM. BUYER WILL PROMPTLY REIMBURSE SELLER OR THE GUARANTOR FOR ANY ARBITRATION FILING FEE, HOWEVER, IN THE EVENT THAT BOTH**

SELLER AND THE GUARANTOR MUST PAY FILING FEES, BUYER WILL ONLY REIMBURSE SELLER'S ARBITRATION FILING FEE AND, EXCEPT AS PROVIDED IN THE NEXT SENTENCE, BUYER WILL PAY ALL ADMINISTRATION AND ARBITRATOR FEES. IF THE ARBITRATOR FINDS THAT EITHER THE SUBSTANCE OF THE CLAIM RAISED BY SELLER OR THE GUARANTOR OR THE RELIEF SOUGHT BY SELLER OR THE GUARANTOR IS IMPROPER OR NOT WARRANTED, AS MEASURED BY THE STANDARDS SET FORTH IN FEDERAL RULE OF PROCEDURE 11(B), THEN BUYER WILL PAY THESE FEES ONLY IF REQUIRED BY THE AAA OR FORUM RULES. SELLER AND THE GUARANTOR AGREE THAT, BY ENTERING INTO THIS AGREEMENT, THEY ARE WAIVING THE RIGHT TO TRIAL BY JURY. BUYER, SELLER OR ANY GUARANTOR MAY BRING CLAIMS AGAINST ANY OTHER PARTY ONLY IN THEIR INDIVIDUAL CAPACITY, AND NOT AS A PLAINTIFF OR CLASS MEMBER IN ANY PURPORTED CLASS OR REPRESENTATIVE PROCEEDING. FURTHER, BUYER, SELLER AND ANY GUARANTOR AGREE THAT THE ARBITRATOR MAY NOT CONSOLIDATE PROCEEDINGS FOR MORE THAN ONE PERSON'S CLAIMS, AND MAY NOT OTHERWISE PRESIDE OVER ANY FORM OF A REPRESENTATIVE OR CLASS PROCEEDING, AND THAT IF THIS SPECIFIC PROVISION DEALING WITH THE PROHIBITION ON CONSOLIDATED, CLASS OR AGGREGATED CLAIMS IS FOUND UNENFORCEABLE, THEN THE ENTIRETY OF THIS ARBITRATION CLAUSE SHALL BE NULL AND VOID. THIS AGREEMENT TO ARBITRATE IS GOVERNED BY THE FEDERAL ARBITRATION ACT AND NOT BY ANY STATE LAW REGULATING THE ARBITRATION OF DISPUTES. THIS AGREEMENT IS FINAL AND BINDING EXCEPT TO THE EXTENT THAT AN APPEAL MAY BE MADE UNDER THE FAA. ANY ARBITRATION DECISION RENDERED PURSUANT TO THIS ARBITRATION AGREEMENT MAY BE ENFORCED IN ANY COURT WITH JURISDICTION. THE TERMS "DISPUTES" AND "CLAIMS" SHALL HAVE THE BROADEST POSSIBLE MEANING.

34. **<u>RIGHT TO OPT OUT OF ARBITRATION</u>. SELLER AND GUARANTOR(S) MAY OPT OUT OF THE ARBITRATION PROVISION ABOVE. TO OPT OUT OF THE ARBITRATION CLAUSE, SELLER AND EACH GUARANTOR MUST SEND BUYER A NOTICE THAT THE SELLER AND EACH GUARANTOR DOES NOT WANT THE CLAUSE TO APPLY TO THIS AGREEMENT. FOR ANY OPT OUT TO BE EFFECTIVE, SELLER AND EACH GUARANTOR MUST SEND AN OPT OUT NOTICE TO THE FOLLOWING ADDRESS BY REGISTERED MAIL, WITHIN 14 DAYS AFTER THE DATE OF THIS AGREEMENT: LEGEND ADVANCE FUNDING II, LLC, 800 BRICKELL AVENUE, SUITE 902, MIAMI, FLORIDA 33131, ATTENTION: CUSTOMER SERVICE.**

Initial Here

Appendix A – List of Fees and Charges

The Agreement provides that Seller shall be liable for the following amounts, in addition to the Purchased Amount of Future Receipts:

1. Origination Fee as set forth on page one. The Origination Fee is deducted from the Purchase Price.

2. Insufficient Funds Fee: $35.

3. Default Fee: the lesser of $5,000 or 25% of amount of undelivered Purchased Amount of Future Receipts at the time of the event of Default.

4. A fee of up to 150% of the actual costs incurred by Buyer associated with the filing, amendment or termination of any UCC filings.

5. All costs of collections, including attorney fees and all costs related to the enforcement of any other remedies available to Buyer if the Seller defaults.

AUTHORIZATION AGREEMENT

FOR AUTOMATED CLEARING HOUSE TRANSACTIONS

[Gerasimos Petratos] ("Seller") hereby authorizes Legend Advance Funding II, LLC ("Buyer") to present automated clearing house (ACH) debits to the following checking account in the amount of fees and other payments due to Buyer from Seller under the terms of that Purchase and Sale of Future Receipts Agreement (the "Agreement") entered into between Seller and Buyer, as it may be amended, supplemented or replaced from time to time. Seller also authorizes Buyer to initiate additional entries (debits and credits) to correct any erroneous transfers. In addition, if an Event of Default (as defined in the Agreement) occurs, Seller authorizes Buyer to debit any and all accounts controlled by Seller or controlled by any entity with the same Federal Tax Identification Number as Seller up to the total amount, including but not limited to, all fees and charges, due to Buyer from Seller under the terms of the Agreement.

Seller agrees to be bound by the Rules and Operating Guidelines of NACHA and represents and warrants that the designated account is established and used primarily for commercial/business purposes, and not for consumer, family or household purposes. Seller authorizes Buyer to contact Seller's financial institution to obtain available funds information and/or to verify any information Seller has provided about the designated checking account and to correct any missing, erroneous or out-of-date information. Seller understands and agrees that any revocation or attempted revocation of this Authorization will constitute an event of default under the Agreement for the Purchase and Sale of Future Receipts. In the event that Seller closes the designated checking account, or the designated checking account has insufficient funds for any ACH transaction under this Authorization, Seller authorizes Buyer to contact Seller's financial institution and obtain information (including account number, routing number and available balance) concerning any other deposit account(s) maintained by Seller with Seller's financial institution, and to initiate ACH transactions under this Authorization to such additional account(s). To the extent necessary, Seller grants Buyer a limited Power of Attorney to take action in Seller's name to facilitate this authorization.

Transfer Funds To/From:

Name of Bank: Citibank

ABA Transit/Routing #: [redacted]0089

Checking Account #: [redacted]8065

This authorization is to remain in full force and effect until Buyer has received all amounts due or that may become due to Buyer under the Agreement.

Seller Information:

Seller's Name: Gerasimos Petratos

Signature of Authorized Representative: _

Print Name: Gerasimos Petratos

Title: Owner

Seller's Tax ID: 30-1177472

Date:

EXCEPTIONAL DELIVERY AND PERFORMANCE ADDENDUM

Legend Advance Funding II, LLC offers a discount for exceptional performance under your Purchase and Sale of Future Receipts Agreement!

Pursuant to your Agreement with us, you are delivering 11.51% of your Future Receipts to us. Your Agreement provides you with the right to obtain an adjustment to the amount that you remit to us each day to reflect your actual Future Receipts from the prior calendar month. We also offer a discount if you elect to deliver the Purchased Amount of Future Receipts according to our exceptional performance schedule:

Exceptional Performance Schedule

Delivery before 30 day	$**32,600.00**
Delivery before 60 day	$**32,600.00**
Delivery before 90 day	$**22,900.00**

Please be advised that this Exceptional Performance Option will be unavailable if:

- The funds come from Legend Advance Funding II, LLC, an affiliate, assignee, or any another funding company in the form of a business loan or a merchant cash advance.
- There has been a modification to your agreement with Legend Advance Funding II, LLC.
- There has been a breach or default of your agreement with Legend Advance Funding II, LLC.

If you are interested in participating in our Exceptional Performance Option, please sign below and return this letter to us.

Agreement of Seller/Business:

Business: Hiteks Solutions, Inc.

Agreed to by: (Signature), its Owner (Title)

Print Name: Gerasimos Petratos

AGREED AND ACKNOWLEDGED:

Signature: Date:

Guarantor

Print Name: **Gerasimos Petratos**

Company Name: **Hiteks Solutions, Inc.**

Address: **447 Broadway Floor 2, New York, New York, 10013**

UNITED STATES DISTRIC COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

THE PEOPLE OF THE STATE OF NEW YORK, by LETITIA JAMES, Attorney General of the State of New York, Plaintiff, v. CITIBANK N.A., Defendant.	Case No. 24 Civ. 0659

COMPLAINT

Plaintiff the People of the State of New York, by Letitia James, the Attorney General of the State of New York, bring this action against Citibank, N.A. ("Citi") and alleges as follows:

INTRODUCTION

1. The rapid growth of online and mobile banking in recent years has placed consumers in the crosshairs of increasingly sophisticated scams. Convincing impersonation scams by text message and over the phone, known as phishing, and mobile device hacks, such as SIM swaps, pose ever-present threats. Through these frauds, scammers gain access to consumers' hard-earned wages, savings, retirement nest eggs, and college funds. Scammers can then use online or mobile banking access to make purchases, transfer money through payment apps such as Zelle or Venmo or by wire transfer, and engage in other unauthorized payment activity.

2. Because scammers execute these frauds and unauthorized payments by electronic means, a landmark consumer protection law known as the Electronic Fund Transfer Act ("EFTA") provides substantial protection. As with credit cards, so long as consumers promptly alert banks

to unauthorized activity, the EFTA limits losses and requires reimbursement of stolen funds. These consumer protections cannot be waived or modified by contract.

3. Banks, as the sophisticated financial institutions that market and offer online and mobile banking directly to consumers, thereby are incentivized by the EFTA to deploy safety measures, security protocols, and other guardrails to prevent scammers from infiltrating online and mobile banking and engaging in unauthorized activity to steal consumer funds.

4. Or so it should be. As alleged herein, however, Defendant Citi has not deployed sufficiently robust data security measures to protect consumer financial accounts, respond appropriately to red flags, or limit theft by scam. Instead, Citi has overpromised and underdelivered on security, reacted ineffectively to fraud alerts, misled consumers, and summarily denied their claims. Citi's illegal and deceptive practices have cost New Yorkers millions.

5. Citi makes online and mobile banking available to consumers, which consumers can access using usernames and passwords, codes, or other security protocols, and through which consumers can review account information, deposit checks, and make electronic payments. In recent years, Citi has connected wire transfer services to consumers' online and mobile banking, providing consumers with direct electronic access to the wire transfer networks.

6. When scammers infiltrate consumers' online or mobile banking to initiate fraudulent wire transfers using this access, two things occur. *First*, scammers electronically instruct Citi to send tens of thousands of dollars or more by wire to third-party banks where scammers have set up dummy accounts. *Second*, scammers electronically instruct Citi to reimburse itself by debiting consumers' bank accounts. These electronic instructions, however, do not come from the actual consumers who are Citi account holders. Under the EFTA, Citi's electronic debits of consumers' accounts are unauthorized and Citi must reimburse all debited amounts.

7. Yet when panicked consumers notify Citi of fraudulent activity on their accounts, there is no mention of the EFTA. Nor did Citi take immediate action in the past to recover amounts it wired out. Instead, Defendant's representatives frequently assure consumers (falsely) that their money and accounts are secure and then instruct consumers to visit their local branches.

8. When consumers arrive at local branches, Defendant's representatives likewise say nothing about the EFTA. They instruct consumers to complete form "Affidavits of Unauthorized Online Wire Transfers," often telling consumers that Citi will not take any action to investigate their fraud claims until the affidavits are executed and notarized. Defendant's representatives also encourage consumers to include details on how they were scammed in those affidavits.

9. Unsuspecting consumers complete these affidavits believing they are necessary for Citi to investigate claims and reclaim their stolen funds. In fact, under cover of these coerced affidavits, Citi treats consumers' claims as subject to narrow commercial laws governing wire transfers rather than the EFTA's robust protections for unauthorized electronic payments. Citi then summarily rejects claims for reimbursement and instead blames consumers, relying on the same information that Defendant's representatives encourage consumers to share with Citi.

10. Citi relies on the Uniform Commercial Code ("UCC"). Under the UCC, banks are not required to reimburse payments for unauthorized wire transfers if they execute wire transfer requests in good faith and subject such requests to commercially reasonable security procedures that are to be negotiated between banks and their sophisticated commercial customers.

11. But consumers negotiate no security procedures with Citi. When consumers sign up for online or mobile banking they must agree to Defendant's online terms and conditions, under which Citi provides consumers with the means to electronically access their accounts. And while Citi promises its online and mobile banking will be safe and secure, the terms and conditions set

out weak security procedures, such as single-factor protocols relying on usernames and passwords, that are readily susceptible to breach by scams such as phishing or SIM swaps.

12. Citi's data security policies and procedures, its efforts to monitor, secure against, and defeat fraudulent activity in real time, and its responses to obvious red flags of identity theft and account takeover are haphazard and ineffective. Among other things:

a. Citi permits scammers to alter contact information, usernames, and passwords, upgrade accounts to access online wire transfer services, and consolidate funds across multiple accounts, all without subjecting to robust scrutiny scammers' subsequent requests to initiate large-dollar wire transfers that will empty consumers' accounts;

b. Citi fails to employ tools that effectively monitor and respond to anomalous consumer or account activity, such as wire transfers that are the first ever involving consumers' accounts, that are for out-of-the-ordinary amounts based on past activity, or that will effectively empty consumers' accounts; and

c. even when alerted to fraudulent activity, Citi does not effectively secure consumers' bank accounts, which remain vulnerable to scammers.

13. The results are devastating. Consumers lose tens of thousands of dollars or more by doing nothing more than clicking on a link in a text that appears to be from a trusted source, providing information on a call with a purported representative of Citi, or answering security questions on a website that looks official. These small acts, done in good faith by consumers who believe they are acting to secure their accounts or prevent fraud, result in large losses in minutes. Depression, shame, embarrassment, extreme stress, and financial strain often follow.

14. Plaintiff alleges that Defendant has violated New York Executive Law § 63(12) by engaging in repeated and persistent illegal conduct by:

Case 1:25-cv-00659 Document 1-11 Filed 01/30/25 Page 5 of 162

a. failing to comply with the EFTA or the UCC in its handling of consumers' notices of fraudulent electronic payment activity (Counts I & IV);

b. failing to apply the EFTA to unauthorized electronic transfers that consolidate funds from multiple accounts into a single account (Count II);

c. employing adhesive online terms and conditions for consumer banking that violate the EFTA's anti-waiver provisions and the EFTA's requirement that contractual terms be clear and readily understandable (Count III);

d. failing to develop, implement, and maintain reasonable safeguards to protect the security, confidentiality, and integrity of consumers' financial account information as required by New York's SHIELD Act (Count V); and

e. failing to maintain a data security program that is appropriately designed to detect, prevent, and mitigate identify theft in response to red flags indicative of possible identity theft, as required by applicable regulations (Count VI).

15. Plaintiff further alleges that Defendant has violated Executive Law § 63(12) and New York General Business Law § 349 by repeatedly and deceptively inducing consumers to enter into agreements setting forth inadequate security procedures, misleading consumers about their rights, depriving consumers of statutory safeguards, falsely promising consumers that their money is secure when it is not, tricking consumers into executing unnecessary affidavits, inflating the likelihood of recovery of stolen funds, and blaming the victims (Counts VII & VIII).

16. The Court should enjoin Defendant from engaging in illegal and deceptive conduct, should order Defendant to hire an independent third party to review its handling of consumers' claims of unauthorized payment activity in connection with fraudulent wire transfers, and should award restitution, disgorgement, damages, penalties, and other relief as appropriate.

PARTIES & JURISDICTION

17. Plaintiff is the People of the State of New York, by their attorney, Letitia James, the New York Attorney General ("OAG") and is authorized to take action to enjoin repeated and persistent fraudulent and illegal conduct under New York Executive Law § 63(12) and deceptive business practices under New York General Business Law ("GBL") § 349.

18. Defendant Citibank, N.A. is a national bank whose principal offerings include investment banking, commercial banking, cash management, trade finance, and e-commerce; private banking products and services; consumer finance, credit cards, and mortgage lending; and retail banking products and services. As of 2022, Citi held more than $1 trillion in deposits, including more than $400 billion in consumer deposits. Defendant is headquartered at 5800 South Corporate Place, Sioux Falls, South Dakota 57108. Defendant is the wholly owned subsidiary of Citigroup, Inc., headquartered at 388 Greenwich Street, New York, New York 10013.

19. Plaintiff has provided Defendant with notice as specified in GBL § 349.

20. This Court has subject-matter jurisdiction over this action because it presents a federal question, 28 U.S.C. § 1331, and because the state-law claims form part of the same case or controversy with those claims that present a federal question, 28 U.S.C. § 1367(a).

21. This Court has personal jurisdiction over Defendant because the causes of action arise from Defendant's contracting with New York residents to supply goods and services in New York and from Defendant's committing of tortious acts within and without New York causing injury to persons or property within New York. Fed. R. Civ. P. 4; CPLR 302.

22. Venue is proper in this district because Plaintiff resides in this district, a substantial amount of the transactions, practices, and courses of conduct at issue occurred within this district, and because Defendant conducts business in this district. 28 U.S.C. § 1391(b)(2).

FACTUAL ALLEGATIONS

I. CONSUMERS TODAY INCREASINGLY FACE HIGHLY SOPHISTICATED SCAMS SEEKING TO INFILTRATE ONLINE AND MOBILE BANKING

23. In 1978, consumer access to wire transfer networks was extremely limited—and continued to be for decades. A 2002 Congressional Research Service report on electronic payment systems in the United States, for example, did not even acknowledge the possibility of consumer use of the wire networks, defining the "primary wire transfer system" as a network that "transfers, disburses, and collects funds for depository financial institutions, corporations, and governmental agencies." And in its tri-annual studies of non-cash payment activity and trends in the United States, the Federal Reserve, as late as 2010, defined consumer or retail payments—as opposed to business or financial institution payments—to exclude wire transfers entirely.

24. The past decade, however, has seen a rapid expansion of widely available internet access, high-speed Wi-Fi, and mobile devices. With this changing environment came the rise of online and mobile banking, through which consumers became accustomed to accessing their bank accounts electronically, reviewing account balances and status online, going paperless, paying bills automatically, and engaging in a wide array of online and mobile banking activity.

25. These trends were further accelerated during the Covid-19 pandemic: one recent report stated that 87% of U.S. adults primarily bank online or on mobile devices.

26. With these shifts, banks began to market and provide electronic payment options directly to consumers, including the ability to seamlessly transfer money among bank accounts online or using mobile devices. Many banks also redesigned their payment systems to provide consumers with electronic access to wire transfer services over the internet or on mobile devices. Citi, for example, advertises to consumers the ability to "conveniently send money" same day by wire transfer and offers to waive wire transfer fees for certain account holders.

27. The result has been an enormous increase in consumer wire activity. According to the Federal Reserve, from 2012 to 2018, consumers' use of wire networks grew at double-digit percentage rates. And while wire transfer volume measured in dollars fell by 2.5% overall from 2015 to 2018, consumer wire transfer volume increased by 20% over the same period.

28. By 2018, consumer wire transfers amounted to more than $4.3 trillion annually, and consumer wire transfers constituted 11% of all wire transfers by transaction.

29. The explosion of online and mobile banking, including the ability to electronically access wire transfer services, has been accompanied by an explosion in frauds through which scammers attempt to infiltrate online or mobile banking to steal consumers' money.

30. One commonly used scam is an impersonation scam, also referred to as "phishing," through which scammers call or send emails or text messages to consumers pretending to be banks or other reputable institutions, such as the government or a well-known business. The purpose of impersonation scams is to trick consumers into providing personal or security information that can be used to fraudulently infiltrate consumer accounts, including online or mobile banking.

31. Phishing scams have grown rapidly over the last several years. In 2021, the FBI reported that these sorts of scams had grown by more than 1,000% from 2017 to 2021. The FTC similarly reported that impersonation scams are a leading source of fraud, amounting to more than 750,000 complaints and losses of more than one billion dollars in 2021 alone.

32. Another commonly used scam targets mobile device subscriber identity modules, or SIMs, that contain unique identifiers for consumers' mobile phones. These "SIM swaps" are done by obtaining personal identifying information via text message or the dark web, after which scammers contact mobile providers to activate new phones with consumers' stolen SIMs and

Case 1:24-cv-00659 Document 1-11 Filed 01/30/25 Page 9 of 162

deactivate consumers' actual phones. Once in control, scammers can reset key apps on devices using text message authentication, including mobile banking and email apps.

33. The goal of these and other similarly sophisticated scams aimed at modern consumers is the same: gaining information sufficient to fraudulently infiltrate online and mobile banking. Scammers then are able to steal consumers' money through various means made available by consumers' banks, including online purchases using virtual debit cards, peer-to-peer payments such as Zelle or Venmo, purchases of gift cards or cryptocurrency, and wire transfers where banks have provided direct electronic access to the wire transfer networks.

34. The FTC reported that in 2022 alone, scammers stole hundreds of millions of dollars from consumers using text messages impersonating banks, delivery services, Amazon, and other common service providers. That same report indicated that the single most frequent party that scammers impersonated over text was consumers' banks.

35. These trends have affected Citi. For example, the number of complaints related to Defendant's handling of claims for fraudulent wire transfers submitted by consumers to the federal Consumer Financial Protection Bureau nearly tripled from 2020 to 2022.

36. And Citi is aware of the increased risks posed by scammers. Defendant's own ads state that "scammers are targeting payment methods that allow them to receive funds very quickly and which are difficult to recover," that "bad players are after your personal information because it's the key to your accounts," and that "phone takeover can put your money at risk."

II. THE ELECTRONIC FUND TRANSFER ACT: LANDMARK CONSUMER PROTECTION LEGISLATION GOVERNING ELECTRONIC PAYMENTS

37. Congress enacted the federal Electronic Fund Transfer Act in 1978, decades before banks provided direct electronic access to wire transfer networks via online or mobile banking, to clarify the rights and liabilities of consumers, banks, and other intermediaries for electronic

transfers of money. The EFTA and its implementing Regulation E ("Reg. E") are landmark protections that shift liability for unauthorized transfers from consumers to banks.

38. The EFTA governs any "electronic fund transfer," referred to herein as an "EFT," which it defines as any transfer of funds that is initiated through an electronic terminal, telephonic instrument, or computer that orders, instructs, or authorizes a financial institution, such as Citi, to debit or credit an account. 15 U.S.C. § 1693a(7). Everyday examples of EFTs include purchases made using debit cards, ATM withdrawals, direct deposits, online bill payments, peer-to-peer payments using mobile apps, transfers among consumers' accounts, and all other debits or credits initiated by computer or mobile device. *Id*; 12 C.F.R. § 1005.3(b)(1).

39. The EFTA and Reg. E protect consumers from unauthorized EFTs and other errors. EFTs are unauthorized when they do not benefit consumers and are made by persons who are not the consumers or other authorized users. 15 U.S.C. § 1693a(12). When scammers fraudulently infiltrate online or mobile banking to electronically execute transactions that cause banks, such as Citi, to move money into or out of consumers' accounts, these are unauthorized EFTs.

40. The EFTA's consumer protections for unauthorized EFTs adhere to a three-tiered structure that is based on when consumers provide notice of unauthorized EFTs to their banks:

a. *First*, when consumers notify banks of unauthorized EFTs within two business days of discovering the EFTs, their losses are capped at $50 or less, and banks must reimburse anything above $50. 15 U.S.C. § 1693g(a).

b. *Second*, when consumers notify banks of unauthorized EFTs within sixty days of discovering the EFTs, their losses are capped at $500, but only if banks prove that those losses would not have occurred had consumers reported the unauthorized EFTs within two business days rather than sixty. 15 U.S.C. § 1693g(a).

c. *Third*, when consumers do not notify banks of unauthorized EFTs within 60 days of discovery the EFTs, their losses are not capped, but only if banks prove that those losses would not have occurred had consumers reported the unauthorized EFTs within sixty business days rather than later. 15 U.S.C. § 1693g(a).

41. The EFTA and Reg. E also require banks to disclose the terms and conditions that apply to EFTs in readily understandable language. 15 U.S.C. § 1693c(a); 12 C.F.R. § 1005.4.

42. Consumer protections in the EFTA and Reg. E, including for unauthorized EFTs, cannot be waived or limited by any agreement, including consumers' deposit agreements, online account agreements, or fund transfer agreements with their banks. 15 U.S.C. § 1693l.

43. The practical result of the EFTA and Reg. E is that banks bear the bulk of losses when consumers' funds are lost due to scammers' large-dollar, unauthorized EFTs. Banks thus are incentivized to prevent unauthorized access to consumers' bank accounts through online or mobile channels, thereby fostering consumer confidence in the electronic banking system.

III. SCAMMERS' USE OF CONSUMERS' ONLINE OR MOBILE BANKING TO EXECUTE WIRE TRANSFERS RESULTS IN UNAUTHORIZED EFTS BY CITI

44. Wire transfers are electronic means of moving money between banks over a secure network. The first wire network was developed by the Federal Reserve as a faster and more secure way to settle amounts owed between banks located in different geographic areas, replacing the need for banks to settle accounts through physical delivery of cash or gold.

45. Over time, the wire networks grew commercially as alternatives for businesses to sending paper instruments such as checks or transporting cash or gold to settle accounts. These transactions were historically done in person, over the phone, or by other means agreed upon between the businesses that accessed the wire transfer networks and their banks.

46. The simplest and most common form of a wire transfer involves four parties: the sender, who wants to send money; the beneficiary, to whom the sender wants to send money; the receiving bank, a bank that receives an instruction to execute a wire transfer (and where the sender often has a bank account); and the beneficiary bank, a bank at which the beneficiary has a bank account. The actual movement of money from the sender to the beneficiary involves several fund transfers, only some of which actually involve the wire transfer networks.

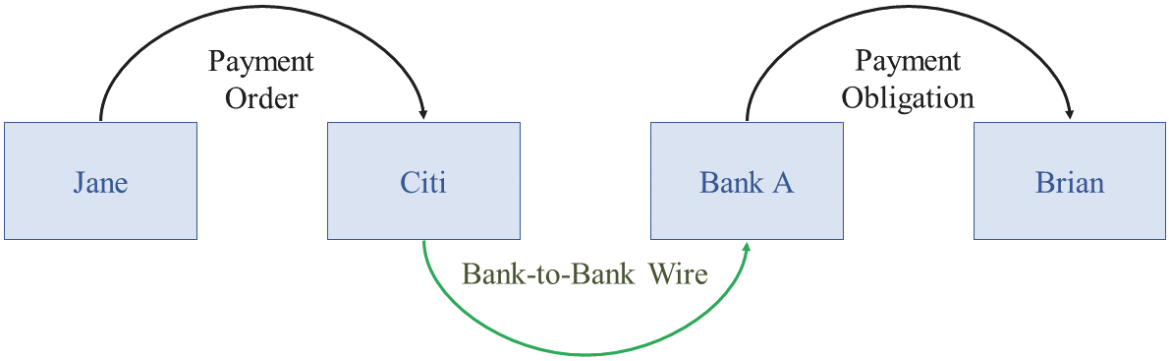
47. The first step is a "Payment Order," which is an instruction sent by the sender to the receiving bank instructing it to pay or cause another bank to pay the beneficiary. U.C.C. § 4-A-103(1)(a). Payment Orders can be sent orally, such as by visiting a local branch to request a wire transfer, electronically, such as online or using a mobile device, or in writing.

48. For example, if Jane, who has a bank account at Citi, wants to send $1,000,000 by wire to Brian, who has a bank account at Bank A, Jane will send a Payment Order to Citi instructing Citi to cause Bank A to pay $1,000,000 into Brian's bank account. Jane is the sender, Citi is the receiving bank, Brian is the beneficiary, and Bank A is the beneficiary bank.

49. When a receiving bank accepts a sender's Payment Order, it sends a new Payment Order, either directly to the beneficiary bank if both banks participate in a common wire network, or through one or more intermediary banks, in which case each bank accepts the prior Payment Order and issues a new Payment Order until the final Payment Order is accepted by the beneficiary bank. The simplest form—transmission of a Payment Order directly from the receiving bank to the beneficiary bank over a wire network—is referred to herein as a "Bank-to-Bank Wire."

50. When a beneficiary bank accepts the final Payment Order, it becomes obligated to pay the amount in question to the beneficiary. U.C.C. § 4-A-404(1). In the example, the chain of

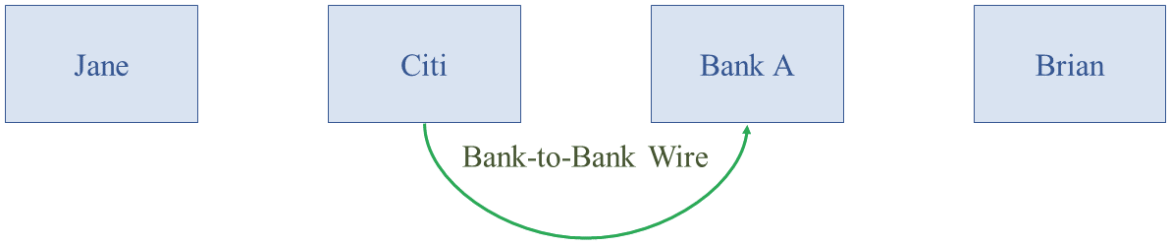
events for Jane to send $1,000,000 by wire to Brian consists of a Payment Order from Jane to Citi, a Bank-to-Bank Wire from Citi to Bank A, and a payment obligation from Bank A to Brian:



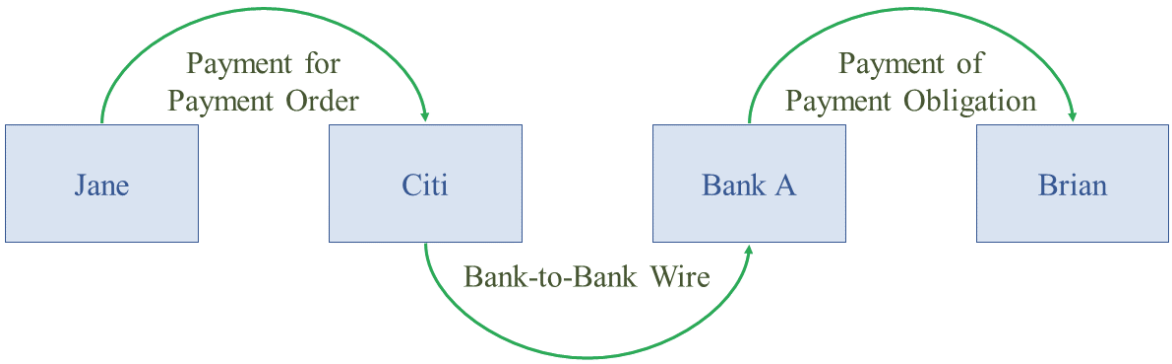
51. Bank-to-Bank Wires are fast and efficient because the participating banks agree to a predetermined set of rules and processes for settlement, netting out obligations across millions of dollars of transfers every day. For example, banks that participate in Fedwire, one of the two primary domestic wire networks, have master accounts with the Federal Reserve. When a receiving bank sends a Payment Order through Fedwire, a Federal Reserve bank will debit the receiving bank's master account and credit the beneficiary bank's master account. Similarly, for banks that participate in the Clearing House Interbank Payments System, or CHIPS, settlement occurs at the end of the day, when CHIPS nets all incoming and outgoing Bank-to-Bank Wires for each bank. Those banks whose outgoing payments exceeded their incoming receipts then immediately send, via Fedwire, funds to cover the shortfall to a CHIPS settlement account. CHIPS then sends those funds to the banks whose incoming receipts exceeded their outgoing payments.

52. As a result of these agreements among the banks who are direct participants in the wire transfer networks, when a beneficiary bank receives a Payment Order from a receiving bank over a wire network, the beneficiary bank need not analyze receiving bank's creditworthiness or assess the likelihood that the receiving bank will pay. The beneficiary bank can simply accept the Payment Order. Today, acceptance of interbank Payment Orders is near instantaneous.

53. A Bank-to-Bank Wire, however, is a movement of money between banks. While initiated by a sender's Payment Order to the receiving bank and resulting in the beneficiary bank's payment obligation to the beneficiary, money in a Bank-to-Bank Wire moves only from a receiving bank to a beneficiary bank (at times through intermediary banks). In the example, no money moves, either from Jane to Citi, or from Bank A to Brian, in the Bank-to-Bank Wire:



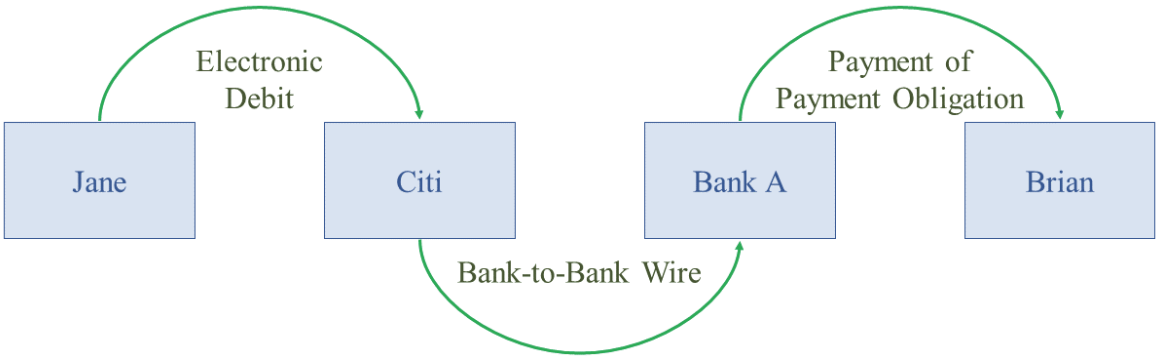
54. Other fund transfers occur in relation to a Bank-to-Bank Wire, but the transfers generally do not take place over the wire networks. In connection with a Bank-to-Bank Wire, the sender is obligated to pay for the initial Payment Order, U.C.C. § 4-A-402(2), while the beneficiary bank, upon accepting the final Payment Order, is obligated to pay the beneficiary, *id*. § 4-A-404(1). In the example, Jane is obligated to pay $1,000,000 to Citi for accepting her initial Payment Order and Bank A is obligated to pay $1,000,000 to Brian when it accepts Citi's Payment Order. But the payments made to satisfy these obligations are independent of the Bank-to-Bank Wire:



55. A sender can pay for a Payment Order in many ways. A sender who submits a Payment Order in-person at a local branch might pay in cash, write a check, or verbally authorize

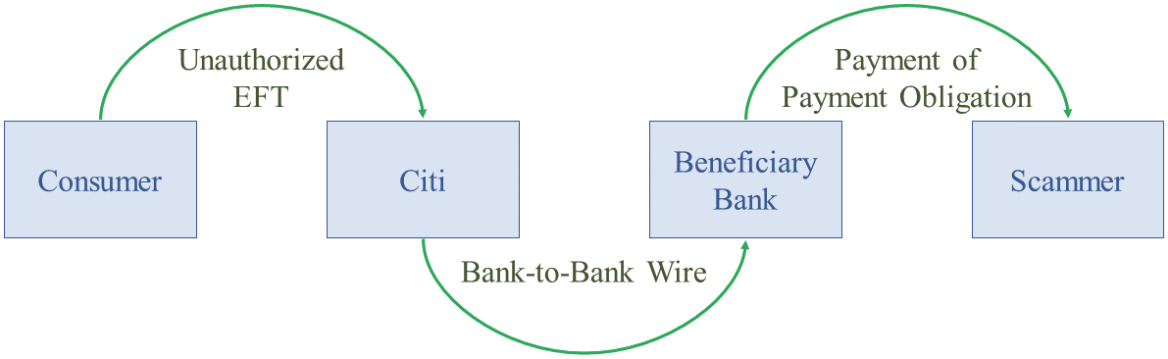
the bank to debit a bank account. A sender who submits a Payment Order in writing might include a check, credit card authorization, or debit authorization with that writing. And a sender who submits a Payment Order electronically might send a credit card or debit authorization.

56. When Citi receives Payment Orders from consumers initiated electronically via online or mobile banking, Citi applies its Agreement for Online Funds Transfers or comparable agreements. These agreements provide that consumers' electronic transfer requests to Citi, such as Payment Orders, also act as electronic authorizations for Citi to debit consumers' bank accounts to pay for the transfers. In the example, when Jane uses online or mobile banking to send her Payment Order to Citi, she also electronically authorizes Citi to debit her bank account:

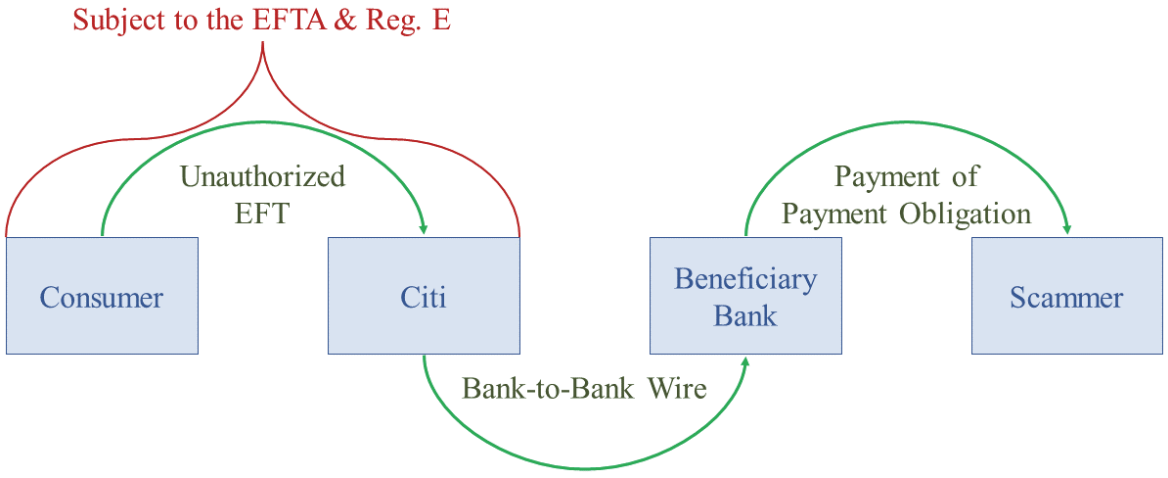


57. But when Citi receives Payment Orders from scammers initiated electronically after infiltrating consumers' online or mobile banking, it is the scammers, and not the consumers, who purport to electronically authorize Citi to debit consumers' bank accounts. These electronic debit authorizations do not come from the affected consumers and the resulting debits do not benefit those consumers. Citi's electronic debits therefore are unauthorized EFTs. In the example, if Brian is not a known party but is instead a scammer who fraudulently infiltrates a consumer's online or mobile banking to electronically send a Payment Order and related debit authorization to Citi, the resulting debit by Citi of the affected consumer's account is an unauthorized EFT:

Case 1:25-cv-00659 Document 1-11 Filed 01/30/25 Page 106 of 162



58. Given the lightning-fast speed at which wire networks operate, scammers' executions of these frauds are nearly instantaneous: tens of thousands of dollars disappear from consumers' bank accounts and in an instant reappear in accounts at beneficiary banks for scammers to steal. And as detailed below, Citi characterizes this complex set of transfers as a single, instantaneous "wire transfer" to confuse, mislead, and deprive affected consumers of their legal rights. But the payment mechanics are clear: each of (i) the unauthorized EFTs that Citi executes to pay itself for the fraudulent Payment Orders, (ii) the Bank-to-Bank Wires between Citi and the beneficiary banks, and (iii) the beneficiary banks' payments into scammers' accounts are independent fund transfers. And each is subject to particular laws, including—with respect to at least the unauthorized EFT from a consumer's account to Citi—the EFTA and Reg. E:



IV. CITI ILLEGALLY ATTEMPTS TO END-RUN THE EFTA AND REG. E BY DECEIVING CONSUMERS & DENYING CLAIMS AS A MATTER OF COURSE

59. When consumers learn that their online or mobile banking has been compromised and notify Citi of stolen funds in connection with scammers' fraudulent Payment Orders and Citi's unauthorized EFTs, Defendant's representatives will lock consumers' bank accounts and instruct consumers to visit their local branches. As a result, investigations are delayed hours or days, providing time for scammers to escape with stolen funds held at beneficiary banks.

60. When consumers visit their local branches, Defendant's representatives state that before Citi will investigate the fraudulent activity or take any other action, consumers must execute and have notarized a form "Affidavit of Unauthorized Online Wire Transfer." These affidavits make no reference to the EFTA, to Reg. E, or to Citi's unauthorized EFTs.

61. When completing these affidavits at local branches, Defendant's representatives often encourage consumers to include specific details regarding how scammers infiltrated their online or mobile banking, at times even filling out the affidavits for consumers. Citi often relies on this information when it later blames consumers and denies their claims.

62. Under the guise of these affidavits, Citi treats consumer claims as solely claims for unauthorized Payment Orders governed by the UCC. Citi does not apply the EFTA to its own unauthorized EFTs initiated electronically by scammers, citing a narrow but inapplicable exclusion for Bank-to-Bank Wires. Citi does not provisionally credit consumers' accounts. Citi does not cap consumers' liability for unauthorized EFTs. And Citi does not treat intra-bank transfers among accounts that provide funds for fraudulent activity as unauthorized EFTs.

63. Citi's investigations that follow submission of affidavits are ineffective, pro forma, and not reasonably tailored to mitigate the security failure that led to the unauthorized EFTs and

consumer losses. Indeed, Defendant's representatives responsible for conducting and completing investigations do not always even speak directly to complaining consumers.

64. These investigations conclude when Citi sends consumers form letters in the mail titled "Decision on Fraud Claim" that refer to an "Unauthorized Wire Claim" and make no mention of the EFTA, Reg. E, or Citi's unauthorized EFT. This typically occurs in 30 to 60 days and receipt of the letter can be the first time that consumers have heard anything from Citi.

65. Defendant's form letters make no reference to the EFTA or Reg. E. The form letters do not describe the scope of the investigation, what actions Citi took, or what evidence Citi relied upon. The form letters merely assert, in one or two sentences, one of a few predetermined grounds for denying claims. These predetermined descriptions of Citi's purported findings include:

- "You did not take adequate steps to safeguard your account. This failure compromised the security of your account information and directly contributed to allowing the transaction(s) in question to take place."
- "Claim was denied due to the fraud reported was caused by providing customer account information or authorization for the transactions that were determined to be a scam."
- "No new information was received or discovered that would change the denial decision."

Citi's form letters do not describe, cite, or append as exhibits any evidence for these predetermined conclusions. Indeed, Citi does not even update the boilerplate language in the first bullet above to reflect whether its investigation involved one or more fraudulent transactions.

66. Other than blaming consumers, Citi's form letters provide no details on the bases for its denials. The letters do not, for example, state what security procedures (discussed below) Citi employed, nor do they provide any evidence that those procedures were followed.

V. CITI APPLIES THE UCC AND NOT THE EFTA TO CONSUMERS' CLAIMS FOR FRAUDULENT WIRE TRANSFERS AND UNAUTHORIZED EFTS

67. Citi treats the Affidavit of Unauthorized Online Wire Transfers it receives solely as claims by consumers for reimbursement for unauthorized Payment Orders under the UCC.

68. Article 4-A of the UCC was adopted after the EFTA and was crafted to not interfere with the EFTA. In particular, Article 4-A expressly provides that it does not apply to transfers that are governed by the EFTA, U.C.C. § 4-A-108(1), and that in the event of any inconsistency between the UCC and the EFTA, the EFTA governs, *id*. § 4-A-108(3). Citi's discarding of the EFTA and Reg. E in favor of the UCC is not consistent with this legal framework.

69. Nor could Citi successfully rely on the UCC to shield itself from liability for these frauds in any event. The UCC generally provides that banks must reimburse customers for unauthorized Payment Orders. U.C.C. § 4-A-204(1). However, banks and their customers can agree upon specific security procedures for verifying Payment Orders that the banks receive. *Id*. § 4-A-201. And if banks can prove that these procedures are commercially reasonable, were followed, and that Payment Orders were accepted in good faith, the UCC provides that the banks need not reimburse customers, even for unauthorized Payment Orders. *Id*. § 4-A-203.

70. Whether particular security procedures are commercially reasonable is determined by a variety of factors, including the circumstances of the customer known to the bank, such as the size, type, and frequency of Payment Orders normally issued by the customer to the bank.

71. The UCC specifies that use of an authorized signature specimen alone is not a sufficient security procedure. Consistent with this approach, legal and policy consensus is that comparable single-factor procedures, such as an online username and password, also are not a commercially reasonable security procedures standing alone. For example, the Federal Financial Institutions Examination Council ("FFIEC"), a federal interagency body that prescribes uniform

procedures for U.S. financial institutions, has publicly cautioned that use of single-factor authentication is inadequate either to safeguard against scammers fraudulently infiltrating customers' online or mobile banking or to prevent widespread payment fraud.

72. Multi-Factor Authentication ("MFA"), as opposed to single-factor authentication, is one available control for financial institutions to prevent fraudulent online or mobile activity. MFA requires more than one distinct authentication factor. The factors are something consumers know (such as usernames and passwords), something consumers have (such as mobile devices), and something consumers are (such as fingerprints or other biometric identifiers).

73. MFA, however, has been shown to be ineffective when used alone. Consumers' email accounts, browsers, and mobile devices are common access points for scammers. Thus, the FFIEC recommends that financial institutions employ layered security approaches, which incorporates multiple preventative, detective, and corrective controls, and which is designed to compensate for potential weaknesses in any one control, including MFA.

74. A critical aspect of layered security is an evaluation of consumers and their account histories, including usage patterns, the frequency of high-dollar transactions, and whether transactions or other recent online behaviors are anomalous. Nacha, the entity formerly known as the National Automated Clearinghouse Association, which manages the ACH payment network, has commented that commercially reasonable, risk-based approaches to security will consider account characteristics and anomalous behavior. When banks identify anomalous behavior or transactions, commercially reasonable and effective controls will prompt the banks to employ more robust procedures to scrutinize and verify electronic payment activity.

75. In addition to MFA, layered security can include a number of other effective controls, such as requiring dual authorization through different access devices, such as a phone

call to a landline and a text message to a mobile device, limits on transaction frequency or size based on prior usage patterns, and the use of enhanced authentication techniques after changes to account types or characteristics, such as account upgrades or changes to passwords.

76. Another aspect of effective layered security is sufficient training and controls for call center and fraud prevention employees. Scammers use engineering and other sophisticated techniques to deceive these employees into resetting passwords or granting scammers access to accounts, including online or mobile banking. Commercially reasonable security procedures are those that employ monitoring and processes to defeat fraudulent transactions in real time.

VI. CITI PROMISES CONSUMERS SAFE AND SECURE ONLINE AND MOBILE BANKING BUT IN FACT EMPLOYS WEAK SECURITY PROCEDURES

77. When consumers open checking or savings accounts with Citi, they must agree to Citi's standard-form client manual for consumer bank accounts. These agreements are not subject to any negotiation. And critically, whatever terms these or other agreements contain, the contracts cannot waive, limit, or modify the core consumer protections provided by the EFTA.

78. Defendant's standard-form client manual for consumer bank accounts requires that Citi verify the authenticity of Payment Orders through direct, personal contact. It contains the following security procedures provision (emphasis added in bold and italics):

> When you place an order for a funds transfer, we will follow a security procedure established for your protection and ours to verify that the transfer has been properly authorized. You understand that the security procedure is designed only to verify the source of the funds transfer instruction and not to detect errors in the content of that instruction or to prevent duplicate transfers. The procedure depends on the means by which you provide instructions to us. ***Unless we agree on another security procedure, you agree that we may confirm the authenticity and content of instructions by placing a call to any authorized signer on your account***. By placing a transfer order, you agree to our use of the applicable security procedure. You agree to be bound by any funds transfer request that Citibank receives and verifies in accordance with the security procedure outlined above.

79. Citi makes a concerted effort to promote online and mobile banking. Its ads say that the bank is "excited to share" online and mobile banking experiences. Citi's website reads: "Online Banking with Citi Made Easy" and promises simple account management, hassle-free fund transfers, and convenient payments, among other features. Citi's website shows consumers how to review account information, deposit checks, and locate ATMs, all online.

80. Citi similarly pushes banking through its mobile app, promising to give consumers "the power of simplicity to manage all your finances, virtually anytime and anywhere!"

81. Citi's efforts to push consumers toward online and mobile banking is a conscious business decision by the bank to compete and drive revenue. Citi has publicly acknowledged that it is "clear that for us at Citi, mobile banking is a significant channel." As one of Citi's regional heads of digital banking states in an online advertisement for Citi's online banking experience, "mobile represents the best opportunity to extend the reach of our services."

82. Central to Citi's efforts to promote online and mobile banking are promises of safe and secure electronic banking experiences. Citi advertises its online banking platform as "an affordable account with a range of convenient Citi digital services," promising that security "is a priority for Citi with 24/7 fraud detection services and security features to keep your account information protected." And Citi represents that it is "constantly working to safeguard your account." It further promises consumers that Citi is "here to keep your card protected."

83. Among its online advertising, Citi represents the following to consumers:

- "As always at Citi, your security is important to us."
- "We, at Citi, consider your security to be the topmost priority."
- "At Citi, we take protecting your account seriously."

84. Despite these promises, when consumers enroll in online and mobile banking with Citi, they must agree to Defendant's adhesive online terms and conditions, which supplant the direct-contact security procedures in the client manual. These revised security procedures are not negotiated with consumers and rely primarily on single-factor authentication—consumers' usernames and passwords—while removing any requirement of direct, personal contact. And many of the potential security procedures that would typically be expected are made entirely discretionary depending on Citi's whims. In particular (emphasis added in bold and italics):

> ***Citi Online has been designed to reduce the possibility of fraud and error by placing the issuance of a User ID and Passwords ("Codes")*** under your control so that accounts may be accessed only upon entry of valid Codes. ***You authorize Citibank to treat any instruction made on Citi Online with valid Codes as if the instructions had been made in writing and signed by you.*** Unless there is substantial evidence to the contrary, Citibank records will be conclusive regarding any access to, or action taken through, Citi Online. You are responsible for maintaining the confidentiality of the Codes and you will not allow any person (including another Citibank customer or your employee) to use the Codes. You agree to inform Citibank promptly of any discrepancies that you discover. ***Citibank will therefore consider any access to Citi Online through use of valid Codes to be duly authorized, and Citibank will carry out any instruction given regardless of the identity of the individual who is actually accessing the system***. You confirm the security system and controls are commercially reasonable and appropriate for you. When you place an order for a funds transfer (including a wire or cable transfer), ***Citibank may follow a security procedure*** established for your protection that ***may entail*** a telephone call or other required contact with you or from you prior to acting upon your instructions. In certain instances, Citibank may also decline to act upon your instructions. Citibank ***may employ other controls*** to verify your identity as a condition of granting access including the collection and use of data that authenticate you or your computer. You agree to these security procedures, and acknowledge that if contacted, either by telephone or electronically, you will act or respond in compliance with requests resulting from these security procedures and will be bound by any resulting transfer or decision not to act upon your instructions or to deny access to persons purporting to be you.

85. The above security procedures in Citi's online terms and conditions appear in the 21st paragraph of dense, legalistic text. And depending on how consumers enroll in online or mobile banking with Citi, they need not scroll past these terms or even open them at all.

86. Nor does Citi encourage consumers to closely review these security procedures. One Citi advertisement that walks through the steps to sign up for electronic banking, for example, shows a consumer scrolling through just a few paragraphs of disclosures while not opening the online account agreement at all—the only place the revised security procedures would appear—before scrolling back up to e-sign the agreement. Another Citi online advertisement shows a consumer registering for Citi's mobile app by opening the lengthy terms and conditions and then clicking "done" before even scrolling to the second paragraph, let alone the twenty-first.

87. Citi's security procedures also do not clearly disclose that Citi is no longer required to make direct, personal contact to verify that Payment Orders are in fact authorized by account holders, even in the presence of red flags. Nor is there any opportunity provided by Citi during the sign-up process for consumers to negotiate alternative procedures, such as the dual authorization protocols or physical tokens that Citi makes available to its commercial customers.

88. Defendant's procedures also contain superficial references to telephone calls, text messages or other controls—the sorts of checks that consumers are used to for anomalous activity on credit cards and other transactions—thereby suggesting that Citi will take similar steps to prevent fraudulent online or mobile banking activity. The procedures do not, however, make clear either that these procedures are discretionary or that by signing up for online or mobile banking consumers have agreed to security procedures that purport to bind them to any actions taken by anyone—even scammers—who have access to consumers' usernames and passwords.

89. Finally, Citi's online terms and conditions purport to alter the legal framework for EFTs in violation of the EFTA's anti-waiver provisions. For example, the terms and conditions provide that Citi may treat EFTs made using consumers' username and password as "authorized" while the EFTA requires persons to have actual authority for authorized EFTs—not just usernames

and passwords. The terms and conditions also alter the burden of proof and Citi's obligations to undertake a reasonable investigation under the EFTA and Reg. E, instead providing that Citi may deem its records "conclusive" in the absence of "substantial" contrary evidence.

VII. CITI'S SECURITY PROCEDURES ARE DISORGANIZED, HAPHAZARD, AND INCAPABLE OF EFFECTIVELY SAFEGUARDING CONSUMER FUNDS

90. While Citi is aware that scammers pose an increasing threat to consumers, the weakened security procedures set out in its electronic banking agreements are utterly ineffective at preventing consumers from falling victim to scams and losing significant sums.

91. When scammers fraudulently infiltrate consumers' online or mobile banking with Citi, the process to execute a Bank-to-Bank Wire online is quick and easy.

92. *First*, scammers must ensure that consumers' online or mobile banking accounts have been linked to the wire transfer networks. If the infiltrated accounts are not linked, scammers can either upgrade account types to those that are linked to the wire networks or can enroll directly in electronic wire transfer services—all of which can be done in moments.

93. *Second*, scammers must create new payees, who are the parties (typically scammers or their co-conspirators) that will act as the beneficiaries in the fraudulent Bank-to-Bank Wires that follow. To do so, scammers enter information (without authorization) into Citi's online or mobile banking platform about the payees, including names and account information.

94. *Third*, scammers must determine the amount of funds available. Where consumers have multiple Citi accounts, such as multiple checking or savings accounts, scammers frequently consolidate funds into one account by making intra-bank transfers, leaving the other accounts with near-zero balances. This avoids any additional scrutiny that might attend the rapid sending of multiple Payment Orders. These intra-bank transfers are done electronically and without triggering any heightened scrutiny, security procedures, or notice to consumers.

95. *Fourth*, scammers must use consumers' online or mobile banking to both send electronic Payment Orders instructing Citi to execute Bank-to-Bank Wires and to electronically authorize Citi—without consumers' knowledge or consent—to debit consumers' accounts.

96. *Fifth*, consistent with the online terms and conditions, Citi may perform whatever security procedures it determines to apply, in its sole discretion. This might include requests for verification via text message to mobile phone numbers that scammers have already SIM swapped, requests for email verification sent to email accounts that scammers have fraudulently infiltrated, or one-time codes sent to the mobile phones of consumers who have been deceived into sharing those codes with scammers pretending to be Citi representatives over the phone.

97. *Sixth*, if Citi accepts scammers' fraudulent Payment Orders, Citi will send new Payment Orders over wire networks to beneficiary banks. Money will then be moved between Citi and the beneficiary bank in the manner predetermined by the wire network. Internal Citi records of these Bank-to-Bank Wires identify Citi's own accounts (not consumers' accounts) as the sources of the funds and the beneficiary bank's own accounts as the recipients.

98. *Seventh*, per its account agreements, Citi will treat scammers' fraudulent Payment Orders as electronic authorizations to debit consumers' accounts to repay itself for the Payment Order, plus fees. Citi will execute unauthorized EFTs from consumers' accounts.

99. The amount of time between when scammers first fraudulently infiltrate online or mobile banking and when funds are stolen can be mere minutes. As a result, scammers' entire fraud can be executed hours, if not days, before consumers discover missing funds.

100. As scammers execute steps one through six above, Citi regularly fails to account for obvious red flags, employs inconsistent approaches to verification, does not react quickly to real-time notices of fraudulent activity, and needlessly delays efforts to recover stolen funds.

A. Citi's Security Procedures Fail to Defeat Fraudulent Payment Orders in the Face of Anomalous Account Activity and Other Clear Red Flags

101. For example, scammers, after fraudulent infiltrating consumers' online or mobile banking, can change passwords for account access. This locks consumers out and ensures that if they notice fraudulent activity in real time they cannot access online or mobile banking to attempt to stop that fraudulent activity. Yet when Citi receives Payment Orders tied to accounts whose passwords were altered hours or even minutes earlier, Citi does not always apply its most robust verification procedures to safeguard against potentially fraudulent Payment Orders. Nor does Citi respond by treating the transaction as an indication of possible identity theft.

102. Citi similarly does not employ its most robust security procedures in the face of other indicators of fraudulent activity, such as Payment Orders involving accounts whose status were recently upgraded, accounts that were recently enrolled in online wire transfer services, or accounts where the username or contact information was recently altered. The presence of these anomalous activities does not automatically trigger the most robust verification procedures that Citi employs or cause Citi to review the accounts in question for possible identity theft.

103. Citi likewise fails to account for intra-bank transfer activity when evaluating new Payment Orders. When scammers use intra-bank transfers to empty accounts and consolidate funds into a single bank account that is then used to send to Citi a large fraudulent Payment Order, Citi's internal procedures does not flag this account activity as suspicious in any way.

104. Citi also does not apply its most robust verification procedures to Payment Orders received within minutes of rejected Payment Orders involving the same accounts. At times Citi cancels fraudulent Payment Orders after it is unable to verify those orders directly—either because Citi is unable to contact consumers directly or because scammers provide inaccurate information when contacted. Yet when scammers submit new Payment Orders minutes later using the same

accounts for the same amounts, no heightened scrutiny is applied. To the contrary, at times Citi employs weaker verification procedures to the subsequent fraudulent Payment Orders.

105. Nor do Citi's security procedures meaningfully account for consumer or account characteristics. Consumers could be Citi account holders for decades, having never sent a Payment Order over years and years of account activity, and yet first-time Payment Orders purporting to be from such consumers do not trigger Citi's most robust verification procedures, nor do such red flags prompt Citi to evaluate whether the account has been subject to identity theft. This is true even when Payment Orders are received hours or minutes after other red flags, such as changes to passwords, preceding intra-bank account transfers, or upgraded account statuses.

106. Citi also does not subject Payment Orders that are anomalous based on consumers' historical account activity, such as Payment Orders for substantial amounts or that will result in near-zero account balances, to its most robust verification procedures as a matter of course.

B. Citi's Security Procedures Do Not Effectively Respond to Notices of Unauthorized Payment Orders or Defeat Ongoing Fraudulent Activity

107. Citi exacerbates its failure to design and implement effective front-end safeguards that identify and defeat fraudulent Payment Orders by employing ineffective processes for consumers who attempt to defeat fraudulent Payment Orders in real time.

108. One security procedure Citi may (in its sole discretion) employ is a simultaneous text message and email describing online activity and asking consumers to respond via text message or click a button in an email confirming or denying the legitimacy of a transaction. If consumers deny the legitimacy, Citi then instructs them to contact its fraud prevention department. But the initial text or email indications of fraud are not sufficient to secure consumers' accounts. While consumers are on (often lengthy) holds waiting for Defendant's representatives to come on

the line, scammers remain able to remove temporary holds and proceed with fraudulent Payment Orders electronically, thereby causing Citi to execute unauthorized EFTs.

109. Frightened and panicked consumers who are being contacted by Citi about fraudulent activity involving large sums, and who reasonably worry that the text messages or emails are themselves scams, at times decide to hang up and call a trusted number (such as the customer service line on their debit cards) or rush to their local branch. Citi itself encourages such precautions, warning consumers: "If you have any doubt, contact the company directly." But calls and visits take time, involving lengthy holds and transfers. Meanwhile, consumers' original responses via text or email that Payment Orders were not legitimate do not prevent scammers from removing holds and successfully sending Payment Orders electronically.

110. When consumers finally do reach Defendant's customer service line, moreover, poorly trained Citi representatives can do little to assist them. First-line representatives for Citi are not always empowered to directly lock accounts or reject Payment Orders. At best, they can transfer consumers to Citi's fraud prevention department, placing them back on hold.

111. Meanwhile, consumers' statements to Defendant's representatives that scammers are attempting to fraudulently send Payment Orders using consumers' bank accounts do not fully secure consumers' accounts. Scammers remain able to satisfy different security procedures working with Defendant's other representatives while consumers remain on hold, after which Citi will accept fraudulent Payment Orders and execute unauthorized EFTs.

112. Even reaching fraud prevention is not always enough. Scammers who have fraudulently obtained access to online or mobile banking can access all available bank accounts. But if consumers alert Citi fraud prevention about suspicious activity on a single account, Citi does not necessarily secure all accessible accounts. In such circumstances, scammers remain able to

Case 1:25-cv-00659 Document 1-1 Filed 01/30/25 Page 30 of 162

execute fraudulent Payment Orders involving consumers' other, unsecured bank accounts during the period before consumers are able to physically visit their local branches.

113. And Citi's instructions that consumers must visit local branches to secure their accounts leaves consumers who are unable to immediately and quickly do so vulnerable and is not an appropriate response to notification of identity theft. Elderly consumers, consumers who may be recovering from medical procedures or are otherwise unable to immediately leave home, consumers who are living in areas where severe weather is ongoing, and consumers who live substantial distances from their closest branch are particularly at risk.

VIII. AFTER CONSUMER FUNDS ARE STOLEN, CITI DECEPTIVELY PROMISES CONSUMERS THAT SAFEGUARDS ARE IN PLACE TO PROTECT THEM

114. Once Citi executes unauthorized EFTs from consumers' accounts to repay itself for scammers' fraudulent Payment Orders, Defendant and its representatives deceive consumers through promises of account security and high prospects of prompt recovery.

115. Defendant's representatives, after instructing consumers to travel to their local branches to transfer funds to new accounts, assure consumers that their accounts have been secured and any fraudulent activity will be blocked. But scammers who retain access to consumers' online or mobile banking can and do defeat blocks and proceed with fraudulent Payment Orders.

116. Defendant's representatives also often reflexively assure consumers that because fraudulent activity caused consumers' losses, consumers will receive their money back.

117. But historically Citi has made no effort to immediately contact beneficiary banks in response to notices of fraudulent activity either to request that stolen funds be frozen or returned. Citi also has required that consumers explicitly request outreach to beneficiary banks before it will do so in real time. As a result, scammers are able to access and withdraw funds held at beneficiary banks even after consumers have provided notices of fraudulent activity to Citi.

118. Nor does Citi automatically initiate investigations or report fraudulent activity to police or law enforcement authorities when consumers first report that activity to Citi. Instead, Defendant's representatives instruct consumers to visit their local branches to report the activity and initiate investigations—which in turn requires consumers to complete, execute, and notarize the required affidavits. If consumers do not take these steps, Citi takes no further action.

119. Finally, even if Citi determines that consumers should be refunded funds stolen in connection with unauthorized Payment Orders initiated through online or mobile banking, Citi merely credits consumers' accounts; it does not always add statutorily required interest.

IX. CITI'S INEPT HANDLING OF POTENTIALLY FRAUDULENT ONLINE ACTIVITY CAUSES SUBSTANTIAL HARM TO NEW YORK CONSUMERS

120. Citi's refusal to adhere to the EFTA's investigation, provisional credit, and reimbursement requirements for the unauthorized EFTs it executes in connection with fraudulent Payment Orders, Defendant's lax security procedures and protocols to detect and defeat fraudulent Payment Orders, and Citi's ineffective monitoring, real-time response, and investigation of notices of fraudulent payment activity, have caused tremendous harm to New York consumers.

121. Scammers have diverted millions of dollars from New York consumers as a direct result of Citi's illegal and deceptive acts and practices. Consumers have lost their life savings, their children's college funds, or even the money needed to support their day-to-day lives.

122. The harm consumers suffer does not end with the lost money. Consumers who have lost substantial amounts due to scams and are unable to recover that money often feel a deep sense of shame or fear. They suffer from increased levels of stress, both from the loss itself and from the inability to understand what investigation is being done on their behalf. And consumers often are forced to turn to costly sources of funds to replace savings built up over decades.

Case 1:25-cv-00659 Document 1-11 Filed 01/30/25 Page 32 of 162

123. Consumer A. Consumer A has been a Citi banking customer for decades. She recalls sending Citi one or two Payment Orders several years ago, before online banking.

124. On October 26, 2021, Consumer A received a text message that appeared to be from Citi. The message requested that Consumer A log onto a website to provide requested information or call her local branch. Consumer A clicked the link to the website, which appeared to be a website affiliated with Citi. Consumer A did not provide any information.

125. Concerned that the message might be a scam, Consumer A called her local branch. Defendant's representative, after Consumer A described the text message and website, responded "Don't worry about it, it happens all the time" and reminded Consumer A that Citi had security protocols in place. Defendant's representative did not place any hold on Consumer A's account, nor did he transfer Consumer A to Defendant's fraud prevention department.

126. Three days later, on October 29, 2021, Consumer A logged onto her email account and discovered that in the span of a few hours that day a scammer had changed her electronic banking password, enrolled her account in online wire transfer services, electronically attempted but failed a $39,999 wire transfer, and electronically executed a $40,000 wire transfer.

127. In particular, account records reflect that at 4:34 p.m. on October 29, 2021, a scammer electronically transferred $70,000 from Consumer A's savings account to her checking account. Consumer A did not make, authorize, or benefit from this intra-bank transfer, nor did she receive any notice of it. Consumer A had retired a few months earlier and the $70,000 was most of her savings. As a result, Consumer A's checking account had a balance of $84,542.63.

128. Account records further reflect that shortly thereafter, Citi accepted a $40,000 Payment Order and, in connection with that fraudulent Payment Orders, Citi executed a $40,000

EFT from Consumer A's Citi checking account, plus an EFT for a $17.50 fee. Consumer A did not make, authorize, or benefit from either the Payment Order or the EFTs.

129. After discovering that $40,017.50 had been removed from her account, Consumer A immediately called Citi. After a long hold, Defendant's representative, hearing Consumer A's story, transferred her to the fraud prevention department. After another long hold, Defendant's representative instructed Consumer A to travel to her local branch.

130. On information and belief, Consumer A's conversations with Defendant's two representatives did not cause Citi to immediately contact the beneficiary bank in the fraudulent Bank-to-Bank Wire to have the $40,000 in stolen funds frozen or recalled.

131. The next morning, Consumer A went to her local branch but found it closed.

132. On the next business day, Consumer A again traveled to her local branch. The branch representatives were not helpful and did not know what number to call to contact the appropriate Citi department for assistance. The branch manager told Consumer A: "We don't handle these things." Eventually, Defendants' representative instructed Consumer A to execute and notarize an Affidavit of Unauthorized Online Wire Transfer, which she did.

133. That same day, Consumer A filed a police report at her local precinct.

134. A few days later, Consumer A called Citi customer service, and eventually was transferred to the fraud prevention department. The fraud prevention representative stated that Citi had not received the affidavit. Consumer A faxed in another copy of the affidavit.

135. Over the next several weeks, Consumer A called Citi customer service repeatedly to inquire on the status of the investigation. During each call, Consumer A was required to repeat her entire story. On at least one of the calls, Defendant's representative stated that a supervisor had approved Consumer A's claim and that she would receive her stolen funds back.

136. Citi subsequently sent Consumer A a December 15, 2021 letter stating: "Claim was denied due to the fraud reported was caused by providing customer account information or authorization for the transactions that were determined to be a scam." Consumer A was never interviewed in connection with any investigation by Defendant.

137. Citi subsequently rejected Consumer A's appeal of the denial of her claim.

138. As of the execution date of this Complaint, Consumer A has not received any of the $40,000 payment or $17.50 fee taken by Citi via EFTs from her account, or interest.

139. Consumer B. Consumer B has been a Citi bank account holder for decades. She does not recall ever sending a Payment Order to Citi.

140. On the evening of March 1, 2022, Consumer B received a communication from a scammer posing as Citi. The scammer stated that Consumer B's Citi bank account was locked and that she would not receive her direct deposit from her employer unless she verified certain personal information on file with Citi. Consumer B responded by providing the requested personal information, believing it was necessary to receive her next direct deposit.

141. Two days later, on March 3, 2022, at 2:00 p.m., Consumer B's home phone rang. She picked up and heard an automated prompt describe a $22,000 wire transfer and request that Consumer B confirm or deny the legitimacy of the transaction. Consumer B pressed the number on her phone to deny the legitimacy of the transaction. She was then placed on hold.

142. Defendant's representative eventually came on the line and Consumer B's husband stated that the $22,000 transaction was not legitimate. Defendant's internal records of this call state: "Client reported fraudulent wire transaction for $22,000."

143. Defendant's internal records reflect that at 2:02 p.m., while Consumer B was on hold, a scammer contacted Citi directly from a phone number that is not associated with Consumer

B to authenticate the fraudulent Payment Order. According to those records, the scammer entered a phone number that did not match Consumer B's records. The scammer was told to hold for a representative but hung up the phone. The Payment Order was then put on hold.

144. Defendant's internal records further reflect that four minutes later, while Consumer B was still on hold, the scammer contacted Citi directly from a phone number that is not associated with Consumer B to authenticate the fraudulent Payment Order. This time the scammer entered a phone number that was a match and—despite Consumer B having pressed the denial on the phone, the scammer's prior authentication failure, and the scammer contacting Citi from a phone number that was not associated with Consumer B—Citi accepted the fraudulent Payment Order.

145. Account records reflect that at 2:10 p.m. on March 3, 2022, Citi accepted a $22,000 Payment Order and, in connection with that fraudulent Payment Order, Citi executed a $22,000 EFT from Consumer B's bank account, leaving it with a near-zero balance. Consumer B did not make, authorize, or benefit from either the Payment Order or the EFT.

146. At 2:16 p.m., six minutes after Citi accepted the fraudulent Payment Order and while her husband was still on the phone, Consumer B logged onto her email account and discovered that in less than one hour before the phone call from Citi the scammer had changed her electronic banking password, added a new payee, enrolled her account in online wire transfer services, and, at 1:59 p.m., electronically sent the $22,000 Payment Order.

147. In response to a 1:59 p.m. "Fraud Alert" email asking her to let Citi "know immediately if you, or anyone you authorized, used your Citibank Checking account" to send a $22,000 Payment Order, Consumer B clicked on the button denying the legitimacy of the Payment Orders. Defendant's internal records state: "Activity denied via email."

148. Despite being informed of the fraudulent Payment Order by telephone and email on March 3, 2022, Citi did not contact the beneficiary bank in the fraudulent Bank-to-Bank Wire to have the $22,000 in stolen funds frozen or recalled until nearly three weeks later.

149. Concerned that Defendant's representative could not assist them over the phone, Consumer B and her husband hung up the phone and traveled together to their local branch. A branch representative contacted Citi fraud prevention to report the fraudulent online activity. The fraud prevention representative stated that the unauthorized transaction had been marked as cancelled, explained that new accounts should be opened, and represented to Consumer B that the $22,000 would be deposited into those new accounts within 24 to 48 hours. Defendant's internal records of this call state: "Wire noted as cancelled, funds should crdt back to the acct."

150. The next day, Friday, March 4, 2022, the branch representative contacted Consumer B and stated that the $22,000 had not yet been deposited into her account. Defendant's representative told Consumer B to check on the status of the funds the following week.

151. On March 7, 2022, Consumer B returned to the branch and Defendant's representative instructed her to execute and notarize an Affidavit of Unauthorized Online Wire Transfer, which she did. Defendant's representative told Consumer B that Citi had not opened any investigation and that Citi would not do so until the affidavit was completed.

152. Citi subsequently sent Consumer B an April 18, 2022 letter stating: "You did not take adequate steps to safeguard your account. This failure compromised the security of your account information and directly contributed to allowing the transaction(s) in question to take place." Consumer B was never interviewed in connection with any investigation by Citi.

153. Consumer C. Consumer C has been a Citi bank account holder for many years.

154. In December 2021, a mortgage servicing firm that serviced loans, including a loan held by Consumer C, experienced a security incident. As a result, an unknown third party obtained personal identifying information, including name, address, loan information, and social security numbers for individuals with loans the firm serviced.

155. Account records reflect that three months later, on March 31, 2022, a scammer electronically transferred $1,887, $4,000, and $10,000 from three of Consumer C's checking and savings accounts to a checking account belonging to Consumer C. Consumer C did not make, authorize, or benefit from these intra-bank transfers, nor did he receive any notice of them. As a result, one of Consumer C's checking accounts had a balance of $38,763.27.

156. Account records reflect that, shortly thereafter, Citi accepted a $37,700 Payment Order and, in connection with that fraudulent Payment Order, Citi executed a $37,700 EFT from Consumer C's checking account, plus an EFT for a $25 fee, leaving it with a near-zero balance. Consumer C did not make, authorize, or benefit from either the Payment Order or the EFTs.

157. Four days later, on April 4, 2022, Consumer C received a letter from the mortgage servicing firm advising him of the security incident and stolen information.

158. Citi subsequently sent Consumer C an April 18, 2022 letter stating: "You did not take adequate steps to safeguard your account. This failure compromised the security of your account information and directly contributed to allowing the transaction(s) in question to take place." Citi subsequently rejected Consumer C's appeal of the denial of his claim.

159. Consumer D. Consumer D has been a Citi bank account holder for twenty-seven years. He does not recall ever sending a Payment Order to Citi.

160. On April 4, 2022, Consumer D received a text message from "citi" stating that he needed to verify certain information. The message contained a link that he clicked.

161. The next day, April 5, 2022, Consumer D's phone rang. He picked up and Defendant's representative asked Consumer D to confirm or deny the legitimacy of a $44,440 wire transfer involving his Citi bank account. Consumer D denied the legitimacy of the transaction. The representative told Consumer D not to worry, that the funds were still in his account, and that Consumer D should travel to a local branch to transfer his funds into new accounts.

162. Defendant's internal records reflect that a scammer accessed Consumer D's mobile banking using a device that Citi had never seen, changed Consumer D's electronic password, and then electronically sent a fraudulent Payment Order. Those records also reflect that Citi assigned a risk score of 1,000 to the scammers' acts (as compared to scores of 1, 33, and 53 for Consumer D's prior usage), flagging risk factors that included a new device, recently linked devices, new IP addresses, login anomalies, and logins large distances from known locations.

163. Despite these red flags and Consumer D's own denial of the legitimacy of the wire transfer, while Consumer D was on the phone with Defendant's representative, the scammer contacted Citi directly to authenticate the fraudulent Payment Order. In violation of protocol, Citi accepted a $44,440 Payment Order and, in connection with that fraudulent Payment Order, Citi executed a $44,440 EFT from Consumer D's savings account, leaving it with a near-zero balance. Consumer D did not make, authorize, or benefit from either the Payment Order or the EFT.

164. When Consumer D subsequently visited his local branch, he discovered for the first time that $44,440 had been stolen from his bank account. Defendant's representative instructed Consumer D to execute and notarize an Affidavit of Unauthorized Online Wire Transfer to initiate an investigation. Defendant's representative completed the text of the affidavit for Consumer D, including a written submission stating: "Client received a fraudulent text message that contained a link. Client clicked on the link, allowing his phone to be compromised."

165. Citi subsequently sent Consumer D an April 29, 2022 letter stating: "You did not take adequate steps to safeguard your account. This failure compromised the security of your account information and directly contributed to allowing the transaction(s) in question to take place." Consumer D was never interviewed in connection with any investigation by Citi.

166. Citi subsequently rejected Consumer D's appeal of the denial of his claim.

167. In June 2023, more than a year later and only after Plaintiff's involvement with Consumer D's matter, Defendant reimbursed Consumer D's bank account with $44,440.

168. Consumer E. Consumer E has been a Citi bank account holder for nearly twenty years. She does not recall ever sending a Payment Order to Citi.

169. On or around April 13, 2022, Consumer E received a text message that appeared to be from Citi. Consumer E clicked the link but did not take any further action.

170. The next day, April 14, 2022, at approximately 12:30 p.m., Consumer E's mobile phone began acting up and it was no longer able to access the mobile network.

171. Later that day, Consumer E logged onto her email account and learned that in the span of less than 30 minutes a scammer had upgraded Consumer E's online account status, enrolled in online wire transfer services, and electronically sent a $50,000 Payment Order to Citi.

172. Account records reflect that on April 14, 2022, Citi accepted a $50,000 Payment Order and, in connection with that fraudulent Payment Order, Citi executed a $50,000 EFT from Consumer E's checking account, leaving it with a near-zero balance. Consumer E did not make, authorize, or benefit from either the Payment Order or the EFT.

173. In response to a 2:01 p.m. "Fraud Alert" email asking her to let Citi "know immediately if you, or anyone you authorized, used your Citibank Checking account" to initiate a $50,000 wire transfer, Consumer E denied the legitimacy of the transaction.

174. After responding to the email, Consumer E called Citi customer service and was placed on a lengthy hold. Defendant's representative, after hearing Consumer E's story, responded that the stolen funds had "already left your account." When Consumer E's boss, who was participating on the call with her permission, asked whether the fraudulent transaction could be reversed, Defendant's representative refused to answer. Defendant's representative then instructed Consumer E to contact Citi's fraud prevention department.

175. Consumer E called the fraud prevention department number and, after another lengthy hold, explained to Defendant's representative that the unauthorized transaction was fraudulent. Defendant's representative instructed Consumer E to visit her local branch.

176. On information and belief, Consumer E's conversations with Defendant's two representatives did not cause Citi to immediately contact the beneficiary bank in the fraudulent Bank-to-Bank Wire to have the $50,000 in stolen funds frozen or recalled.

177. Consumer E later visited her local branch. Defendant's representative instructed her to execute and notarize an Affidavit of Unauthorized Online Wire Transfer, which she did. The affidavit stated that Consumer E's "phone was hack[ed]," among other details.

178. Consumer E also completed a police report at her local precinct.

179. Citi subsequently sent Consumer E a May 11, 2022 letter stating: "You did not take adequate steps to safeguard your account. This failure compromised the security of your account information and directly contributed to allowing the transaction(s) in question to take place."

180. Citi subsequently rejected Consumer E's appeal of the denial of her claim.

181. As of the execution date of this Complaint, Consumer E has not received any of the $50,000 payment taken by Citi via EFT from her account, or interest.

182. Consumer F. Consumer F has been a Citi bank account holder for many years. He does not recall ever sending a Payment Order to Citi.

183. On April 28, 2022, Consumer F received a text message from "citi" stating that his information had not been verified in some time and that his account access "will be disabled unless we have verified" the information. The message contained a link to a website so that Consumer F could "sign on for a safe and secure banking experience."

184. Consumer F clicked on the link and was taken to a website that appeared to be a legitimate Citi website. The website contained the three security questions that Consumer F had answered when setting up online banking with Citi. Believing that this was a legitimate inquiry from Defendant, Consumer F answered the three questions and closed the website.

185. The next day, April 29, 2022, at 1:02 p.m., Consumer F's phone rang. He picked up and heard an automated prompt describe a $7,750 wire transfer and request that Consumer F confirm or deny the legitimacy of the transaction. Defendant's internal records reflect that Consumer F pressed "3" to deny the legitimacy of the transaction. Those records also reflect that Consumer F was told he would be connected to a "fraud specialist" and placed on hold.

186. Defendant's internal records reflect that while Consumer F was on hold, a scammer contacted Citi directly from a phone number that is not associated with Consumer F to authenticate the $7,750 Payment Order and that Citi accepted the fraudulent Payment Order.

187. Account records reflect that at 1:09 p.m. on April 29, 2022, Citi accepted a $7,750 Payment Order and, in connection with that fraudulent Payment Order, Citi executed a $7,750 EFT from Consumer F's checking account, leaving it with a balance of less than $75. Consumer F did not make, authorize, or benefit from either the Payment Order or the EFT.

Case 1:25-cv-00659 Document 1-11 Filed 01/30/25 Page 43 of 162

188. Defendant's internal records also reflect that the scammer electronically sent the fraudulent Payment Order at 12:56 p.m. One minute later, Defendant sent a text message and email to Consumer F requesting verification of the transfer.

189. Consumer F first saw the text message from Defendant while still on hold following the automated call. The text message referred to a $7,750 transaction and Consumer F became concerned that either he had not stopped the fraudulent online activity by pressing 3 on his phone or that the automated call itself might be fraudulent. Consumer F hung up the phone and called the Citi customer service line on the back of his debit card. After a hold of approximately 50 minutes, Defendant's representative, after hearing Consumer F's story, stated that Citi should be able to stop the unauthorized transaction and instructed Consumer F to visit his local branch.

190. Defendant's internal records reflect that at 2:29 p.m. that same day, Consumer F first opened Defendant's "Fraud Alert" email requesting verification of the transaction and that he immediately "confirmed fraud." Those records also reflect that Citi took no action in response to this email response because "case status is resolved"—*i.e.*, the fraudulent Payment Order had already been accepted by Citi. Despite the telephonic denial, the notice of fraud by phone, and the email denial, Citi took no steps to contact the beneficiary bank in the fraudulent Bank-to-Bank Wire to have the $7,750 in stolen funds frozen or recalled for several hours.

191. Consumer F traveled to his local branch. Defendant's representative instructed him to execute and notarize an Affidavit of Unauthorized Wire Transfer, which he did.

192. Consumer F contacted Citi multiple times per week for the next several weeks but did not receive any updates on his stolen funds. Finally, on or around May 17, 2022, Defendant's representative informed Consumer F that Citi never received an affidavit.

193. That same day, Consumer F again traveled to his local branch to execute and notarize another affidavit, which he submitted along with a written dispute.

194. Weeks later, Citi sent Consumer F a letter stating: "You did not take adequate steps to safeguard your account. This failure compromised the security of your account information and directly contributed to allowing the transaction(s) in question to take place."

195. Citi subsequently rejected Consumer F's appeal of the denial of his claim.

196. In June 2023, more than a year later and only after Plaintiff's involvement with Consumer F's matter, Defendant reimbursed Consumer F's bank account with $7,750.

197. Consumer G. Consumer G has been a Citi bank account holder for decades.

198. On April 29, 2022, Consumer G received a text message that purported to be from Citi. The text message stated that fraudulent activity had been identified on Consumer G's Citi account and asked him to click a link to review the activity. Consumer G clicked the link, his phone began acting up, and it was no longer able to access the mobile network.

199. Email and account records reflect that, shortly after Consumer G's phone began acting up on April 29, 2022, and in the span of less than an hour, a scammer upgraded Consumer G's online account status, enrolled in online wire transfer services, and electronically transferred $9,000 from his savings account to his checking account. As a result of this intra-bank transfer, Consumer G's checking account had a balance of just over $27,000. Consumer G did not make, authorize, or benefit from this intra-bank transfer, nor did he receive any notice of it.

200. Defendant's internal records reflect that, an hour later, the scammer electronically sent three Payment Orders using Consumer G's savings account for $75,000, $75,000, and $68,000 to Citi. Together, had these Payment Order been accepted and had Citi executed EFTs in the same amounts, the unauthorized EFTs would have nearly emptied Consumer G's savings account.

201. Defendant's internal records further reflect that Citi sent "Fraud Alert" emails to Consumer G requesting verification of the Payment Orders. Those records also reflect that the scammer fraudulently authenticated one of the $75,000 Payment Orders by illicitly accessing Consumer G's email app on his hacked phone but did not respond to the "Fraud Alert" emails for the other $75,000 Payment Order or the $68,000 Payment Order.

202. Account records reflect that at 2:05 p.m. on Friday, April 29, 2022, shortly after the SIM swap, Citi accepted a $75,000 Payment Order and, in connection with that fraudulent Payment Order, Citi executed a $75,000 EFT from Consumer G's savings account. Consumer G did not make, authorize, or benefit from either the Payment Order or the EFT.

203. Defendant's internal records reflect that, more than 90 minutes later, the scammer electronically sent two additional Payment Orders using Consumer G's savings account in slightly smaller amounts of $70,000 and $60,000, as replacements for the prior $75,000 and $68,000 Payment Orders that had not been executed. Citi then received a phone call from the scammer regarding these fraudulent Payment Orders that resulted in a suspicious caller referral. Citi's fraud prevention department reviewed the referral and rejected the Payment Orders.

204. Despite the suspicious call referral and block on Consumer G's savings account, Citi did not place a hold on Consumer G's checking account at the time, nor did Citi immediately contact the beneficiary bank in the prior fraudulent $75,000 Bank-to-Bank Wire.

205. Account records reflect that two hours later, at 6:05 p.m., Citi accepted a $27,000 Payment Order and, in connection with that fraudulent Payment Order, Citi executed a $27,000 EFT from Consumer G's checking account, leaving it with a near-zero balance. Consumer G did not make, authorize, or benefit from either the Payment Order or the EFT.

206. Less than an hour later, at approximately 6:30 p.m., Consumer G visited his mobile carrier's store. He was told that his SIM had been reassigned to a different mobile device without his authorization. Consumer G obtained a letter from his carrier confirming the SIM swap.

207. Shortly after his mobile phone's SIM was fixed, Consumer G received numerous text messages from Defendant referring to the two executed transactions and four attempted but unexecuted transactions that had occurred during the prior several hours.

208. Consumer G immediately contacted Citi's customer service line at the number on the back of his debit card. After a lengthy hold, Defendant's representative, after hearing Consumer G's story, transferred Consumer G to Citi's fraud prevention department.

209. After another hold, Defendant's representative stated that Consumer G's account had been "frozen," that the fraudulent transaction would not go through, and that no money had been lost. The representative instructed Consumer G to travel to his local branch.

210. The next business day, Monday, May 2, 2022, Consumer G traveled to his local branch where he discovered, for the first time, that two transactions had been executed using his accounts in the amounts of $75,000 and $27,000. At the branch, Defendant's representative told to Consumer G "not to worry" because the transactions were fraudulent.

211. Defendant's branch representative also instructed Consumer G to execute and notarize two Affidavits of Unauthorized Online Wire Transfer, which he did.

212. That same day, Consumer G completed a police report at his local precinct.

213. Despite being informed of the fraudulent activity by Consumer G on April 29, 2022, Defendant Citi did not contact the beneficiary banks in the Bank-to-Bank Wire to have either the $75,000 or $27,000 frozen or recalled until May 4, 2022, five days later.

214. Citi subsequently sent Consumer G two May 11, 2022 letters, each stating: "Claim was denied due to the fraud reported was caused by providing customer account information or authorization for the transactions that were determined to be a scam."

215. Citi subsequently rejected Consumer G's appeals of the denials of his claims. Consumer G submitted his mobile carrier's letter in connection with those appeals.

216. After contact by Plaintiff's office regarding Consumer G's matter, Defendant acknowledged in writing that its suspicious caller referral should have resulted in the securing of Consumer G's checking account in addition to his savings account. In June 2023, and only after Plaintiff's involvement with the matter, Defendant reimbursed Consumer G's checking account with $27,000. As of the execution date of this Complaint, Consumer G has not received any of the $75,000 payment taken by Citi via EFT from his savings account, or interest.

217. Consumer H. Consumer H has been a Citi bank account holder for thirty-plus years. She does not recall ever sending a Payment Order to Citi.

218. On July 6, 2022, Consumer H reviewed her bank accounts with Citi and found a message stating that her account was suspended due to fraudulent activity and instructing her to call a phone number. Consumer H called the identified number and a scammer answered, stated that he was a representative of Citi, and identified himself as James.

219. The scammer told Consumer H that he would be sending her codes from Citi to verify certain account activity and asked Consumer H to read the codes to him over the phone. Over the next 90 minutes, the scammer used codes read by Consumer H, who believed she was providing codes to secure her Citi bank accounts and prevent fraudulent activity, to change Consumer H's electronic banking password and create a new payee. At no time during the phone call did either Consumer H or the scammer discuss any transfers of money.

220. The next day, July 7, 2022, Consumer H discovered that $35,000 had been stolen from her bank accounts when she checked her account balances online. She immediately contacted Defendant's customer service line and was placed on a lengthy hold. Defendant's representative, after hearing Consumer H's story, instructed her to visit her local branch.

221. Account records reflect that at 1:37 and 1:38 p.m. the prior day—while Consumer H was on the phone with the scammer—the scammer electronically transferred $3,544.18, $5,169.19 and $6,091.44 from three of Consumer H's savings accounts to her checking account, leaving each savings account with a $0 balance. Consumer H did not make, authorize, or benefit from these intra-bank transfers, nor did she receive any notice of them. As a result of the three intra-bank transfers, Consumer H's checking account had a balance of $36,031.95.

222. Defendant's internal records reflect that, about an hour after the scammer changed Consumer H's electronic banking password, the scammer electronically sent a $35,000 Payment Order to Citi. Those same records reflect that Citi attempted to verify the Payment Order by an automated phone call to Consumer H, which went unanswered. At 2:07 p.m., after Consumer H did not respond to the verification attempt, Citi rejected the $35,000 Payment Order.

223. Five minutes later, at 2:12 p.m., Citi's fraud prevention department called Consumer H and left a voicemail seeking to "confirm recent online activity." The voicemail did not reference the rejected Payment Order for $35,000 or the intra-bank transfers.

224. Defendant's internal records further reflect that, at 2:25 p.m., the scammer electronically sent an identical $35,000 Payment Order to Citi. Those same records also reflect that, in response, Citi attempted to verify the Payment Order by email and text message sent at 2:27 p.m. Consumer H has never seen any such email and phone records she obtained from her mobile carrier do not reflect any text messages sent or received at 2:27 p.m.

225. Account records reflect that, despite Defendant's prior inability to verify a $35,000 Payment Order or contact Consumer H by phone, at 2:29 p.m. on July 6, 2022, Citi accepted a $35,000 Payment Order and, in connection with that fraudulent Payment Order, Citi executed a $35,000 EFT from Consumer H's checking account, leaving it with a near-zero balance. Consumer H did not make, authorize, or benefit from either the Payment Order or the EFT.

226. Despite being informed of the fraudulent activity by Consumer H over the phone on July 7, 2022, Citi did not contact the beneficiary bank in the fraudulent Bank-to-Bank Wire to have the $35,000 in stolen funds frozen or recalled until July 8, 2022, a full day later.

227. After returning home from out of state, Consumer H traveled to her local branch. Defendant's representative instructed Consumer H to execute and notarize an Affidavit of Unauthorized Online Wire Transfer Activity, which she did.

228. Consumer H also completed a police report at her local precinct.

229. Approximately 60 days later, Citi sent Consumer H a September 15, 2022 letter stating: "Claim was denied due to the fraud reported was caused by providing customer account information or authorization for the transactions that were determined to be a scam." Consumer H was never interviewed in connection with any investigation by Citi.

230. Citi subsequently rejected Consumer H's appeal of the denial of her claim.

231. As of the execution date of this Complaint, Consumer H has not received any of the $35,000 taken by Citi via EFT from her account, or interest.

232. Consumer I. Consumer I has been a Citi bank account holder for nearly thirty years. She does not recall ever sending a Payment Order to Citi.

233. Consumer I is a retired senior subsisting on social security. In July of 2022, she had saved up approximately $15,613, which she kept in a Citi bank account.

234. In early July 2022, Consumer I received a text message about a package being sent by Federal Express. Consumer I was in fact awaiting a delivery, and she clicked the link provided in the text message. Consumer I was directed to a website where she filled in the requested information and then landed on a screen requesting a $3.00 fee payment, which she made.

235. Concerned that the text message may have been a scam, Consumer I contacted Citi and asked that her current debit card be cancelled and that a new one be sent.

236. On July 12, 2022, at or around 6:30 p.m. and shortly after receiving her new debit card, Consumer I received a phone call from a scammer claiming to be from Citi. The scammer stated that Consumer I was supposed to receive a new debit card, which made Consumer I believe the scammer was legitimate. The scammer then told Consumer I that a fraudulent charge had already been made using her new card and that her account needed to be secured.

237. At the scammer's request, Consumer I provided the card number to the scammer. The scammer then told her that she would receive a code from Citi to secure the account and asked her to read the code back. Consumer I received a code and read it back over the phone.

238. While on the phone with the scammer, Consumer I attempted to log into her Citi online account but was not able to do so. She then checked her email account and first saw emails from Citi confirming a password change and the addition of a new payee.

239. Consumer I immediately hung up the phone and called the Citi customer service number on the back of her phone. After a hold of approximately 30 minutes, a representative came on the line and Consumer I stated that her account had been taken over by a scammer, asked for the account balance, and requested that the account be blocked. Defendant's representative responded that the account balance was $15,613. Consumer I replied "great" and requested that the representative immediately block any account activity. Defendant's representative then replied

that he did not have the ability to block the account but would transfer Consumer I. Consumer I pleaded not to be transferred or be re-identified, but she was placed on hold.

240. Consumer I remained on hold for approximately 20 minutes while crying. Account records reflect that while on this hold—after having told Defendant's representative that a scammer had fraudulent infiltrated her electronic banking—Citi accepted a $15,000 Payment Order and, in connection with that fraudulent Payment Order, Citi executed a $15,000 EFT from Consumer I's bank account, leaving it with a near-zero balance. Consumer I did not make, authorize, or benefit from either the Payment Order or the EFT.

241. Defendant's representative who next came on the line stated: "Thank you very much for calling Citi how can I help you?" Consumer I immediately explained that a scammer had illicitly accessed her online or mobile banking and was trying to wire money. The representative responded that two or three attempts had been made and that "your wire just went out."

242. Consumer I demanded that Defendant's representative immediately contact the beneficiary bank in the fraudulent Bank-to-Bank Wire to freeze or recall the stolen funds. Defendant's representative responded that "we don't do that" and that Citi "has a procedure."

243. On information and belief, Consumer I's conversations with Defendant's two representatives did not cause Citi to immediately contact the beneficiary bank in the fraudulent Bank-to-Bank Wire to have the $15,000 in stolen funds frozen or recalled.

244. Consumer I hung up and called the beneficiary bank directly. The beneficiary bank's representative told Consumer I that the bank could not take any action because she was not an account holder and the bank had not received any recall request from Citi.

245. Consumer I later traveled to her local branch. Defendant's representative instructed her to execute and notarize an Affidavit of Unauthorized Online Wire Transfer, which she did.

246. Citi later sent Consumer I an August 1, 2022 letter stating: "You did not take adequate steps to safeguard your account. This failure compromised the security of your account information and directly contributed to allowing the transaction(s) in question to take place."

247. In October 2022, and only after Plaintiff's involvement with Consumer I's matter, Defendant reimbursed Consumer I's bank account with $15,000, but without interest.

248. Consumer J. Consumer J has been a Citi bank account holder for thirty-plus years. She does not recall ever sending a Payment Order to Citi.

249. On August 11, 2022, Consumer J received a call on her mobile phone that displayed on her phone as Citi. When she answered, a scammer stated that he was a Citi representative and identified himself as Gerald. The scammer asked Consumer J whether she had attempted two transactions in Georgia, and Consumer J responded that she had not. The scammer stated that Consumer J's debit card would be cancelled and that a new debit card would be issued.

250. The scammer then suggested that Consumer J set up two-factor authentication for her account and offered to assist. Consumer J agreed, and the scammer stated that he would be sending her codes to verify certain account activity and asked Consumer J to read the codes over the phone. The scammer then used codes read by Consumer J to change her electronic banking password and electronically send three Payment Orders for $49,300, $49,200, and $48,800 to Citi. During the call, the scammer thanked Consumer J for being a Citi customer and identified a recent transaction at a local grocery store (a real transaction) as the likely source of the account hack. At no time did either Consumer J or the scammer discuss any transfers of money.

251. Defendant's internal records reflect that Citi attempted to verify the three fraudulent Payment Orders by making direct, personal contact with Consumer J, but that Citi was unable to make contact directly with Consumer J. Citi rejected the three Payment Orders.

252. Defendant's internal records further reflect that, after these rejected Payment Orders, the scammer changed the username for Consumer J's electronic banking.

253. Despite a change in password, three rejected Payment Orders, and a change in username, all in succession in a short period, account records reflect that later that same day the scammer submitted and Citi accepted two Payment Orders in the amounts of $9,800 and $9,700 and, in connection with those fraudulent Payment Orders, Citi executed two EFTs in those same amounts from Consumer J's bank accounts, leaving each account with a near-zero balance. Consumer J did not make, authorize, or benefit from either the Payment Orders or the EFTs.

254. Shortly before 10:30 a.m. the next day, August 12, 2022, Consumer J received a delivery from Federal Express but it did not include a new debit card. Because she had expected to receive a new card, Consumer J called Citi's customer service line shortly before 11:00 a.m. During this call, Consumer J described her interactions the prior day with the scammer and asked if a new debit card had gone out. After placing Consumer J on a hold, Defendant's representative stated that a new card had not gone out and told Consumer J that she "would handle it."

255. At no time during this call did Defendant's representative mention any change in password, any change in username, or the Payment Orders (either the three rejected Payment Orders or the two accepted and executed Payment Orders). Defendant has acknowledged in writing that this call should have prompted further inquiry by Citi but did not.

256. Following her call with Citi customer service, Consumer J separately contacted Defendant's fraud prevention number. After another lengthy hold, she again described her interactions the prior day with the scammer. Defendant's representative told Consumer J that transfers had been executed using her accounts and instructed her to travel to her local branch to close her accounts and open new accounts to avoid further losses.

257. Account records further reflect that on August 12, 2022, at 11:54 a.m. and 12:46 p.m.—after Consumer J's call describing the scam to Defendant's representative who could have seen three rejected Payment Orders, two accepted Payment Orders, and two large EFTs but said and did nothing—Citi accepted two Payment Orders in the amounts of $9,900 and $9,897 and, in connection with those fraudulent Payment Order, Citi executed two EFTs in those amounts from Consumer J's Citi bank accounts, leaving each with a near-zero balance. Consumer J did not make, authorize, or benefit from either the Payment Orders or the EFTs.

258. On information and belief, Consumer J's conversations with Defendant's two representatives did not cause Citi to immediately contact the beneficiary bank in the fraudulent Bank-to-Bank Wire to have any of the approximately $40,000 in stolen funds frozen or recalled.

259. That same day, August 12, Consumer J traveled to her local branch. Defendant's representative instructed her to execute and notarize an Affidavit of Unauthorized Online Wire Transfer, which she did. The affidavit stated that Consumer J supplied codes to a scammer.

260. On August 16, 2022, Consumer J completed a police report at her local precinct.

261. Nearly 60 days later, Citi sent Consumer J four October 7, 2022 letters, each stating: "Claim was denied due to the fraud reported was caused by providing customer account information or authorization for the transactions that were determined to be a scam." Consumer J was never interviewed in connection with any investigation by Defendant.

262. In March 2023, seven months later, only after Plaintiff's involvement with Consumer J's matter, and after initially denying that Consumer J spoke with Citi before Citi accepted the two August 12, 2022 fraudulent Payment Orders, Defendant reimbursed Consumer J's four bank accounts with $9,800, $9,700, $9,900 and $9,897, but without interest.

Case 1:25-cv-00659 Document 1-1 Filed 01/30/25 Page 54 of 162

CAUSES OF ACTION

FIRST CAUSE OF ACTION
Executive Law § 63(12) (Illegality)
(EFTA & Reg. E – Unauthorized Debits)

263. Plaintiff repeats and realleges the allegations in paragraphs 1 to 262 above.

264. New York's Executive Law § 63(12) authorizes Plaintiff to seek injunctive and other equitable relief when any individual or business engages in repeated and persistent illegal conduct in the carrying on, conducting, or transaction of business in the state of New York.

265. Under the EFTA and Reg. E, Citi, in response to a notice of an unauthorized EFT, must conduct an investigation, provisionally credit a consumer's account if Citi does not complete the investigation within 10 days, and refund all lost amounts in excess of (i) $50 if notice was provided within two business days of the consumer becoming aware of the unauthorized transfer or (ii) $500 if notice was provided within sixty days of the consumer becoming aware of the unauthorized transfer. 15 U.S.C. §§ 1693f, 1693g; 12 C.F.R. § 1005.6(b). With the exception of these liability thresholds based on the timing of notice provided, "a consumer incurs no liability from an unauthorized electronic fund transfer." 15 U.S.C. § 1693g(e).

266. An EFT is any transfer that "is initiated through an electronic terminal, telephonic instrument, or computer or magnetic tape so as to order, instruct, or authorize a financial institution to debit or credit an account." 15 U.S.C. § 1693a(7). An EFT is unauthorized when the EFT is "initiated by a person other than the consumer without actual authority to initiate such transfer and from which the consumer receives no benefit." *Id*. § 1693a(12).

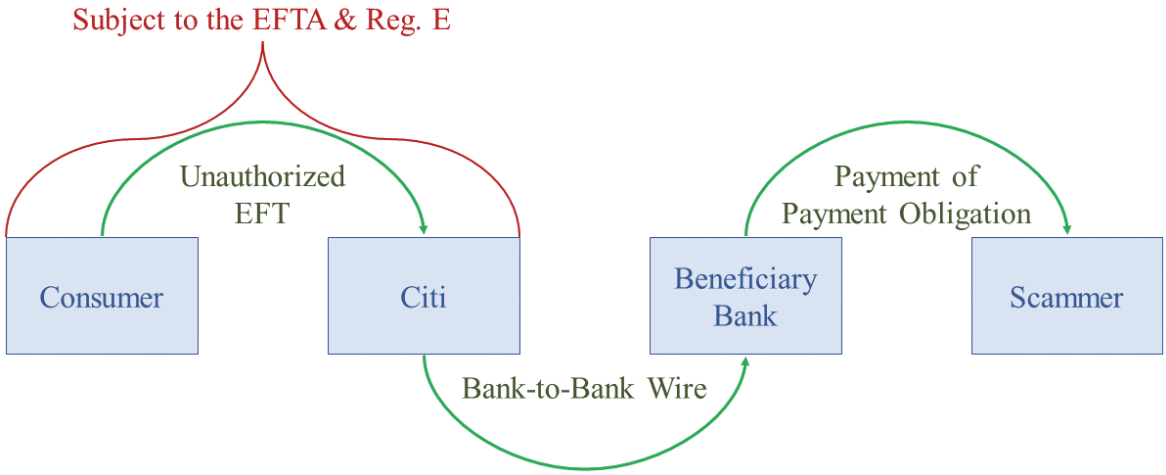
267. Citi has offered consumers online and mobile banking and has connected these services to wire transfer networks. As a result, Citi has provided consumers, through usernames and passwords, codes sent by text message, mobile apps, or a combination thereof, the ability to

electronically initiate wire transfers by sending Payment Orders directly to Citi, and the ability to fund those wire transfers by electronically authorizing Citi to debit their accounts.

268. Scammers have illicitly infiltrated New York consumers' online or mobile banking with Citi, including but not limited to those of Consumers A through J, and used this electronic access to wire transfer networks to send Payment Orders to Citi, which Citi accepted.

269. By sending fraudulent Payment Orders using computers or mobile devices, scammers have purported to electronically authorize Citi to debit consumers' bank accounts to pay itself for those Payment Orders, which Citi has done. Citi did not execute these debits by Fedwire, CHIPS, or means of any other service that transfers funds held at either Federal Reserve banks or depository institutions. Citi's electronic debits from consumers' accounts were EFTs.

270. Citi's execution of EFTs resulted from scammers having fraudulently infiltrated consumers' online or mobile banking and purporting to electronically authorize Citi to debit consumers' accounts without actual authority. Consumers have not benefitted from these EFTs. Citi's electronic debits from consumers' accounts were unauthorized EFTs:



271. Citi's handling of unauthorized EFTs initiated using compromised consumer online or mobile banking access has violated the EFTA and Reg. E in at least the following respects:

a. having required submissions of executed and notarized affidavits before investigating consumers' notices of unauthorized payment activity;

b. having failed to provisionally credit consumers' bank accounts within ten days of consumers' notices of unauthorized payment activity; and

c. having refused to reimburse consumers' bank accounts with the amount of stolen funds in excess of $50 or $500 where consumers provided notice of unauthorized payment activity within two or sixty business days of discovery, respectively.

272. By reason of the conduct alleged herein, Defendant has engaged in repeated and persistent illegal conduct in violation of Executive Law § 63(12).

SECOND CAUSE OF ACTION
Executive Law § 63(12) (Illegality)
(EFTA & Reg. E – Unauthorized Intra-Bank Transfers)

273. Plaintiff repeats and realleges the allegations in paragraphs 1 to 262 above.

274. New York's Executive Law § 63(12) authorizes Plaintiff to seek injunctive and other equitable relief when any individual or business engages in repeated and persistent illegal conduct in the carrying on, conducting, or transaction of business in the state of New York.

275. Under the EFTA and Reg. E, Citi, in response to a notice of an unauthorized EFT, must conduct an investigation, provisionally credit a consumer's account if Citi does not complete the investigation within 10 days, and refund all lost amounts in excess of (i) $50 if notice was provided within two business days of the consumer becoming aware of the unauthorized transfer or (ii) $500 if notice was provided within sixty days of the consumer becoming aware of the unauthorized transfer. 15 U.S.C. §§ 1693f, 1693g; 12 C.F.R. § 1005.6(b). With the exception of these liability thresholds based on the timing of notice provided, "a consumer incurs no liability from an unauthorized electronic fund transfer." 15 U.S.C. § 1693g(e).

276. An EFT is any transfer that "is initiated through an electronic terminal, telephonic instrument, or computer or magnetic tape so as to order, instruct, or authorize a financial institution to debit or credit an account." 15 U.S.C. § 1693a(7). An EFT is unauthorized when the EFT is "initiated by a person other than the consumer without actual authority to initiate such transfer and from which the consumer receives no benefit." *Id*. § 1693a(12).

277. In advance of sending fraudulent Payment Orders, scammers have fraudulently infiltrated consumers' online or mobile banking to consolidate funds from multiple accounts into one account. Scammers have consolidated funds before sending Payment Orders to avoid needing to send multiple Payment Orders, thereby limiting the potential for consumers to notice and take action to stop fraudulent activity and limiting exposure to anti-fraud security measures. Citi's subsequent acceptance of fraudulent Payment Orders and execution of unauthorized EFTs resulted in losses of funds that would otherwise not have been available in the aggregate amount.

278. Scammers who have initiated intra-bank transfers did so electronically through online or mobile banking without authorization from consumers whose funds were in the accounts. These intra-bank transfers among consumers' accounts were unauthorized EFTs.

279. Citi's handling of unauthorized intra-bank EFTs in connection with fraudulent Payment Orders has violated the EFTA and Reg. E in at least the following respects:

a. having required submission of executed and notarized affidavits before investigating consumers' notices of unauthorized payment activity;

b. having failed to provisionally credit consumers' bank accounts within ten days of consumers' notices of unauthorized payment activity; and

c. having refused to reimburse consumers' bank accounts with the amount of stolen funds in excess of $50 or $500 where consumers provided notice of unauthorized payment activity within two or sixty business days of discovery, respectively.

280. By reason of the conduct alleged herein, Defendant has engaged in repeated and persistent illegal conduct in violation of Executive Law § 63(12).

THIRD CAUSE OF ACTION
Executive Law § 63(12) (Illegality)
(EFTA & Reg. E – Illegal Agreements)

281. Plaintiff repeats and realleges the allegations in paragraphs 1 to 262 above.

282. New York's Executive Law § 63(12) authorizes Plaintiff to seek injunctive and other equitable relief when any individual or business engages in repeated and persistent illegal conduct in the carrying on, conducting, or transaction of business in the state of New York.

283. The EFTA and Reg. E require banks who offer EFT services to consumers to disclose the terms and conditions of those services in "clear and readily understandable" language. 12 C.F.R. § 1005.4(a)(1); 15 U.S.C. § 1693c(a). The EFTA further provides that banks' terms and conditions cannot waive or alter the rights conferred by statute. 15 U.S.C. §1693l.

284. When consumers signed up for online or mobile banking with Citi they were required to agree to Defendant's online terms and conditions. The terms and conditions are adhesive and not subject to any negotiation between consumers and Citi.

285. Citi's online terms and conditions have violated the EFTA and Reg. E by failing to describe in clear and readily understandable terms the security protocols that Citi will actually deploy to prevent unauthorized EFTs initiated via online or mobile banking.

286. Citi's online terms and conditions also have violated the EFTA and Reg. E by altering federal consumer protections and rights in at least the following respects:

a. having improperly narrowed the scope of unauthorized EFTs by contractually defining any EFT initiated through online or mobile banking using usernames and passwords as an authorized EFT even if not made with actual authority;

b. having altered Citi's burden of proof by contractually providing that Citi may treat its own internal records and documents as conclusive evidence; and

c. having altered the scope of a reasonable investigation by Citi into notices of unauthorized EFTs provided to Citi by consumers.

287. By reason of the conduct alleged herein, Defendant has engaged in repeated and persistent illegal conduct in violation of Executive Law § 63(12).

FOURTH CAUSE OF ACTION
Executive Law § 63(12) (Illegality)
(UCC Violations)

288. Plaintiff repeats and realleges the allegations in paragraphs 1 to 262 above.

289. New York's Executive Law § 63(12) authorizes Plaintiff to seek injunctive and other equitable relief when any individual or business engages in repeated and persistent illegal conduct in the carrying on, conducting, or transaction of business in the state of New York.

290. Under Article 4-A of the UCC, Citi cannot refuse to refund payments for unauthorized Payment Orders unless Citi accepted the Payment Orders in good faith and in compliance with commercially reasonable security procedures and any instructions of its customers restricting acceptance of payment orders. U.C.C. § 4-A-202(2).

291. Citi has the burden of establishing that it is more probable than not that it acted in good faith and in compliance with the security procedures. U.C.C. § 4-A-105(g).

292. Under Article 4-A of the UCC, if Citi determines that its customers' funds were stolen in connection with unauthorized Payment Orders that were not enforceable, Citi "shall

refund any payment . . .and shall pay interest on the refundable amount calculated from the date the bank received payment to the date of the refund." U.C.C. § 4-A-204(1).

293. Citi has failed to employ commercially reasonable security procedures in connection with its handling of Payment Orders sent electronically in the following respects:

a. Citi's online terms and conditions have incorporated single-factor authentication protocols to verify Payment Orders sent electronically instead of layered security, including MFA, algorithmic monitoring of consumer and account behavior, mechanisms to identify high-risk transactions or anomalous behavior that trigger strengthened procedures, transaction limitations based on frequency, volume, and repeat activity, and training to ensure effective real-time responses to potential fraud, all of which are the hallmarks of commercially reasonable security procedures;

b. Citi has failed to materially alter and employ its most robust verification procedures and protocols in response to anomalous activity that should have indicated suspicious or fraudulent activity, including Payment Orders that: (i) were received within hours of changes to consumers' electronic banking passwords; (ii) were received within hours of changes in consumers' online account type or status; (iii) were received within hours of consumers first enrolling in online wire transfer services; (iv) would have, if accepted and Citi executed EFTs from consumers' accounts in the same amounts, resulted in a near-zero balances in consumers' bank accounts; (v) were received following intra-bank transfers from consumers' other bank accounts that left near-zero balances in those other bank accounts; (vi) were the first or one of the first ever sent by consumers after several years of account activity; and (vii) were received within hours of similar Payment Orders that had been cancelled or were unable to be verified; and

c. Citi has not had sufficient controls and has not trained employees to respond effectively in real-time to reject fraudulent Payment Orders in response to consumers' timely instructions to limit such activity. Specifically: (i) notices of fraudulent activity to Defendant's customer service representatives have not secured consumers' bank accounts such that scammers could no longer successfully execute fraudulent Payment Orders; (ii) long hold times on phone communications after consumers' notices of fraudulent activity have slowed consumers' efforts to secure accounts; (iii) notices of fraudulent activity via telephonic dial or email have not secured consumers' bank accounts such that scammers could no longer successfully execute fraudulent Payment Orders; and (iv) requirements to travel to local branches to secure accounts have left consumers' bank accounts vulnerable to scammers' fraudulent activity.

294. Citi has not acted in good faith or in compliance with its customers instructions in connection with its handling of Payment Orders sent electronically in the following respects:

a. Citi has accepted Payment Orders in the face of one or more of the red flags identified in the preceding paragraph, all of which are common indicators of potentially fraudulent activity that should trigger robust verification protocols;

b. Citi has accepted Payment Orders after consumers had provided notice that those Payment Orders were unauthorized and the result of fraudulent activity; and

c. Citi has substantially delayed contacting beneficiary banks to freeze or recall consumers' stolen funds after notice of fraudulent activity.

295. In addition, Citi's standard-form denial letters, which have appended no evidence, have described no findings, and have followed wholly inadequate investigations that often have not included basic interviews with affected consumers, have not satisfied Citi's burden to prove

Case 1:25-cv-00659 Document 1-1 Filed 01/30/25 Page 62 of 162

that it was more probable than not that it (i) acted in compliance with security procedures, (ii) acted in good faith, or (iii) adhered to consumers' instructions regarding Payment Orders.

296. Finally, where Citi has determined that it was obligated to refund consumers under Article 4-A in connection with scammers' fraudulent Payment Orders, Citi has replaced the lost funds in consumers' bank accounts but often has not included any interest.

297. By reason of the conduct alleged herein, Defendant has engaged in repeated and persistent illegal conduct in violation of Executive Law § 63(12).

FIFTH CAUSE OF ACTION
Executive Law § 63(12) (Illegality)
(SHIELD Act & GBL § 349)

298. Plaintiff repeats and realleges the allegations in paragraphs 1 to 262 above.

299. New York's Executive Law § 63(12) authorizes Plaintiff to seek injunctive and other equitable relief when any individual or business engages in repeated and persistent illegal conduct in the carrying on, conducting, or transaction of business in the state of New York.

300. New York's SHIELD Act requires businesses that own or license computerized data that includes private information of New York residents, including financial account information, to develop, implement, and maintain reasonable safeguards to protect the security, confidentiality, and integrity of that private information. GBL § 899-bb(2). This includes, among other obligations, implementation of reasonable (i) administrative safeguards to both identify reasonably foreseeable internal and external risks and train and manage employees in its security program, *id*. §§ 899-bb(2)(b)(ii)(A)(2)–(4), and (ii) technical safeguards to detect, prevent, and respond to attacks or system failures, *id*. § 899-bb(2)(b)(ii)(B)(3).

301. Failure to comply with the SHIELD Act is deemed a violation of GBL § 349 and Plaintiff is empowered to bring an action on behalf of the People of New York to enjoin such violations and obtain civil penalties under GBL § 350-d. GBL § 899-bb(2)(d).

302. Citi owns or licenses computerized data that includes private information of New York residents, including financial account information belonging to Consumers A through J.

303. Citi has failed to adopt reasonable administrative and technical safeguards, and to identify and respond to the reasonably foreseeable risks posed by scammers accessing financial account information, including as to Consumers A through J. Citi has failed to adopt appropriate layered security, including MFA, algorithmic monitoring of consumer and account behavior, mechanisms to identify high-risk transactions or anomalous behavior that trigger strengthened procedures, or transaction limitations based on frequency, volume, and repeat activity.

304. Citi has failed to train and manage employees to respond to consumers' notice of fraudulent online or mobile banking access or unauthorized payment activity, including:

a. not training employees to secure bank accounts such that scammers could no longer engage in unauthorized activity following verbal notice over the phone;

b. not training employees to not place consumers on long telephonic holds following verbal notice over the phone;

c. not training employees to secure bank accounts such that scammers could no longer engage in unauthorized activity following electronic notice;

d. not training employees to reject all Payment Orders after consumers had provided notice that those Payment Orders were unauthorized and were the result of scammers fraudulent access to online or mobile banking; and

e. training employees to instruct consumers to travel to local branches to secure bank accounts such that scammers could no longer engage in unauthorized activity.

305. Citi has failed to implement technical safeguards to detect, prevent, and respond to either scammers' infiltration of online or mobile banking or scammers' fraudulent payment

activity, thereby compromising consumers' financial account information. Citi also has not responded effectively but instead has accepted large-dollar Payment Orders following anomalous account activity, including (i) changes to consumers' usernames or passwords; (ii) changes in consumers' online account type or status; (iii) enrollments in online wire transfer services; and (iv) transfers from consumers' other bank accounts that left near-zero balances in those accounts.

306. By reason of the conduct alleged herein, Defendant has engaged in repeated and persistent illegal conduct in violation of Executive Law § 63(12).

SIXTH CAUSE OF ACTION
Executive Law § 63(12) (Illegality)
(Red Flag Rule)

307. Plaintiff repeats and realleges the allegations in paragraphs 1 to 262 above.

308. New York's Executive Law § 63(12) authorizes Plaintiff to seek injunctive and other equitable relief when any individual or business engages in repeated and persistent illegal conduct in the carrying on, conducting, or transaction of business in the state of New York.

309. The Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003 rule (the "Red Flag Rule") is a joint final rule adopted on November 9, 2007 by, among other federal agencies, the Federal Trade Commission, 16 C.F.R. § 681.1, and the Office of the Comptroller Currency, 12 C.F.R. § 41.90.

310. The Red Flag Rule applies to "financial institutions," which is defined by reference to the federal Consumer Credit Protection Act, 15 U.S.C. § 1681 *et seq*. 16 C.F.R. § 681.1(b)(7); 12 C.F.R. § 41.90(b)(7). The term "financial institution" means a State or National bank, a State or Federal savings and loan association, and other enumerated entities. 15 U.S.C. § 1681a(t).

311. The Red Flag Rule applies to covered accounts, which are accounts that financial institutions offer or maintain, primarily for personal, family, or household purposes, that involve

or are designed to permit multiple payments or transactions, including checking accounts and savings accounts. 16 C.F.R. § 681.1(b)(3)(i); 12 C.F.R. § 41.90(b)(3)(i).

312. The Red Flag Rule requires financial institutions that offer or maintain covered accounts to establish an identity theft prevention program that is designed to detect, prevent, and mitigate identify theft, including the detection and appropriate response to Red Flags, 16 C.F.R. § 681.1(d)(2)(ii)–(iii); 12 C.F.R. § 41.90(d)(2)(ii)–(iii), and to ensure that the identity theft prevention program is periodically updated to reflect changes in risks to customers posed by identify theft, 16 C.F.R. § 681.1(d)(2)(iv); 12 C.F.R. § 41.90(d)(2)(iv).

313. A Red Flag is a pattern, practice, or specific activity that indicates the possible existence of identity theft. 16 C.F.R. § 681.1(b)(9); 12 C.F.R. § 41.90(b)(9).

314. Citi is a financial institution subject to the Red Flag Rule. Citi offers and maintains covered accounts, including accounts belonging to Consumers A through J.

315. Citi has failed to ensure that Defendant's identify theft prevention program detects and responds appropriately to Red Flags in at least the following respects:

a. not detecting as Red Flags or responding appropriately to prevent large-dollar Payment Orders that were electronically transmitted within hours of changes to consumers' electronic banking passwords;

b. not detecting as Red Flags or responding appropriately to prevent large-dollar Payment Orders that were electronically transmitted within hours of changes in consumers' online account type or status;

c. not detecting as Red Flags or responding appropriately to prevent large-dollar Payment Orders that were electronically transmitted within hours of consumers first enrolling in online wire transfer services;

d. not detecting as Red Flags or responding appropriately to prevent large-dollar Payment Orders that would have, if Citi executed EFTs from consumers' accounts in the same amounts, resulted in a near-zero balances in consumers' bank accounts;

e. not detecting as Red Flags or responding appropriately to prevent large-dollar Payment Orders that were electronically transmitted after transfers from consumers' other bank accounts that left near-zero balances in those other bank accounts;

f. not detecting as Red Flags or responding appropriately to prevent large-dollar Payment Orders that were received within hours of similar Payment Orders that had been cancelled or were unable to be verified;

g. not detecting as Red Flags or responding appropriately to prevent large-dollar Payment Orders that were electronically transmitted in connection with multiple Red Flags identified in the preceding subparagraphs; and

h. not responding appropriately to mitigate financial and other harms caused by identity theft in response to Red Flags identified in any preceding subparagraphs.

316. By reason of the conduct alleged herein, Defendant has engaged in repeated and persistent illegal conduct in violation of Executive Law § 63(12).

SEVENTH CAUSE OF ACTION
Executive Law § 63(12) (Fraud)

317. Plaintiff repeats and realleges the allegations in paragraphs 1 to 262 above.

318. New York's Executive Law § 63(12) authorizes Plaintiff to seek injunctive and other equitable relief when any individual or business engages in repeated and persistent fraud in the carrying on, conducting, or transaction of business in the state of New York.

319. Citi has engaged in fraudulent practices in its account administration and handling of unauthorized EFTs and Payment Orders sent electronically in at least the following respects:

a. having enticed consumers to enroll in online and mobile banking by stressing the security of electronic banking and by creating the impression that online and mobile banking were no less secure than in-person banking when in fact enrollment in online or mobile banking resulted in less security, including adoption of security procedures for Payment Orders sent electronically that did not rely on direct, personal verification but instead employed a single-factor verification mechanism and which permitted Citi, at its sole discretion, to choose from other weak security procedures (or none) that did not effectively defeat unauthorized Payment Orders;

b. having misrepresented consumers' rights and obligations with respect to unauthorized EFTs, including by failing to immediately investigate notices of unauthorized EFTs and failing to provisionally credit consumers' bank accounts;

c. repeatedly having represented that bank accounts were secure and directing consumers to visit local branches when in fact the bank accounts were not safe from scammers, Defendant's representatives often did not secure or even have the ability to secure consumers' accounts, and scammers retained the ability to access online or mobile banking and successfully send fraudulent Payment Orders electronically by satisfying alternative security procedures;

d. having required consumers who provided notice of unauthorized EFTs to execute affidavits asserting claims for unauthorized wire transfers;

e. repeatedly having told consumers that no action could be taken, including any investigation, unless consumers executed affidavits;

f. having encouraged consumers to complete affidavits that describe the circumstances that led to scammers illicitly accessing online or mobile banking under the

pretense of needing affidavits to initiate investigations to recover consumers' funds, at a time when consumers were under severe duress, but then used information provided by consumers to deny consumers' fraud claims;

g. having not immediately attempted to recall funds sent to beneficiary banks following notice of fraudulent activity, delaying for days or even weeks, often after having indicated that funds lost as a result of fraud would be returned; and

h. having represented in its standard form denials for what Citi misleadingly refers to as "unauthorized online wire transfers" that consumers acted improperly—such as not taking "adequate steps to safeguard" accounts or "providing customer account information" in responses to scams—as bases to deny any obligation by Citi to reimburse, which falsely led consumers to believe that their own actions were relevant and deprived them of their legal rights to recover stolen funds.

320. By reason of the conduct alleged herein, Defendant has engaged in repeated and persistent fraudulent conduct in violation of Executive Law § 63(12).

EIGHTH CAUSE OF ACTION
Executive Law § 63(12) (Illegality)
(GBL § 349)

321. Plaintiff repeats and realleges the allegations in paragraphs 1 to 262 above.

322. New York's Executive Law § 63(12) authorizes Plaintiff to seek injunctive and other equitable relief when any individual or business engages in repeated and persistent illegal conduct in the carrying on, conducting, or transaction of business in the state of New York.

323. New York's General Business Law prohibits deceptive acts and practices in the conduct of any business, trade, or commerce in the state of New York. GBL § 349(a).

324. Citi has engaged in deceptive practices in its account administration and handling of unauthorized EFTs and Payment Orders sent electronically in at least the following respects:

a. having enticed consumers to enroll in online and mobile banking by stressing the security of electronic banking and by creating the impression that online and mobile banking were no less secure than in-person banking when in fact enrollment in online or mobile banking resulted in less security, including adoption of security procedures for Payment Orders sent electronically that did not rely on direct, personal verification but instead employed a single-factor verification mechanism and which permitted Citi, at its sole discretion, to choose from other weak security procedures (or none) that did not effectively defeat unauthorized Payment Orders;

b. having misrepresented consumers' rights and obligations with respect to unauthorized EFTs, including by failing to immediately investigate notices of unauthorized EFTs and failing to provisionally credit consumers' bank accounts;

c. repeatedly having represented that bank accounts were secure and directing consumers to visit local branches when in fact the bank accounts were not safe from scammers, Defendant's representatives often did not secure or even have the ability to secure consumers' accounts, and scammers retained the ability to access online or mobile banking and successfully send fraudulent Payment Orders electronically by satisfying alternative security procedures;

d. having required consumers who provided notice of unauthorized EFTs to execute affidavits asserting claims for unauthorized wire transfers;

e. repeatedly having told consumers that no action could be taken, including any investigation, unless consumers executed affidavits;

f. having encouraged consumers to complete affidavits that describe the circumstances that led to scammers illicitly accessing online or mobile banking under the

pretense of needing affidavits to initiate investigations to recover consumers' funds, at a time when consumers were under severe duress, but then used information provided by consumers to deny consumers' fraud claims;

g. having not immediately attempted to recall funds sent to beneficiary banks following notice of fraudulent activity, delaying for days or even weeks, often after having indicated that funds lost as a result of fraud would be returned; and

h. having represented in its standard form denials for what Citi misleadingly refers to as "unauthorized online wire transfers" that consumers acted improperly—such as not taking "adequate steps to safeguard" accounts or "providing customer account information" in responses to scams—as bases to deny any obligation by Citi to reimburse, which falsely led consumers to believe that their own actions were relevant and deprived them of their legal rights to recover stolen funds.

325. By reason of the conduct alleged herein, Defendant has engaged in repeated and persistent illegal conduct in violation of Executive Law § 63(12).

DEMAND FOR RELIEF

WHEREFORE, Plaintiff respectfully requests that the Court issued an order and judgment under Executive Law § 63(12) and General Business Law § 349:

a. permanently enjoining Defendant, its agents, trustees, employees, successors, heirs, and assigns; and any other person under their direction or control, whether acting individually or in concert with others, or through any corporate or other entity or device through which one or more of them may now or hereafter act or conduct business, from engaging in the fraudulent and illegal practices alleged herein;

b. ordering Defendant to provide an accounting of all consumers whose claims for monetary losses in connection with unauthorized Payment Orders and debit authorizations were denied by Defendant in the last six years;

c. appointing an independent third party paid for by Defendant to review the accounting to identify every consumer who was harmed by Defendant's fraudulent and illegal practices alleged herein;

d. ordering Defendant to provide restitution and damages to all injured consumers, whether known or unknown, at the time of the decision and order;

e. ordering Defendant to disgorge all profits from the fraudulent and illegal practices alleged herein;

f. directing Defendant, under General Business Law § 350-d, to pay a civil penalty of $5,000 to the State of New York for each violation of General Business law § 349;

g. awarding to Plaintiff, under CPLR 8303(a)(6), costs in the amount of $2,000; and

h. granting such other and further relief as the Court deems just and proper.

Dated: January 30, 2024

Respectfully submitted,

LETITIA JAMES
Attorney General of the State of New York

By: */s/ Christopher L. Filburn*
Christopher L. Filburn
Assistant Attorney General
Bureau of Consumer Frauds & Protection
28 Liberty Street, 20th Floor
New York, New York 10005
Tel.: 212.416.8303
Email: christopher.filburn@ag.ny.gov

Of counsel:

Jane M. Azia
Bureau Chief

Laura J. Levine
Deputy Bureau Chief

SUPREME COURT OF THE STATE OF NEW YORK
COUNTY OF NEW YORK

Attorneys: Company: Salzano, Jackson & Lampert PH: (646) 863-1883
Address: 275 Madison Avenue, 35th Floor New York, NY 10016

Hiteks Solutions, Inc. Plaintiff V. Citibank, N.A.; John Does 1-5; and ABC Corporations 1-5; Defendants	**Index Number:** 655775/2024 **Date Filed:** 10/30/2024 **Client's File No.:** **Court/Return Date:**

STATE OF NEW YORK, COUNTY OF NEW YORK, SS.:

AFFIDAVIT OF SERVICE

Reginald Hunter, being sworn says:
Deponent is not a party herein is over the age of 18 years and resides in the State of New York.

On **December 10, 2024**, at **11:18 AM** at **388 Greenwich Street, New York, NY 10013,** Deponent served the within **Summons, Complaint and Notice of Electronic Filing**

The index number and the filing date of the action were endorsed upon the face of the papers so served herein.
On: **Citibank, N.A.** , Defendant therein named.

☐ **#1 INDIVIDUAL**
By delivering a true copy of each to said recipient personally; Deponent knew the person so served to be the person described in as said recipient therein.

☐ **#2 SUITABLE AGE PERSON**
By delivering thereat a true copy of each to **(Vice President)** a person of suitable age and discretion. Said premises is recipient's:[] actual place of business / employment [] dwelling house (usual place of abode) within the state.

☐ **#3 AFFIXING TO DOOR**
By affixing a true copy of each to the door of said premises which is subjects
[] actual place of business / employment [] dwelling house (usual place of abode) within the state. Deponent was unable with due diligence to find subject or person of suitable age and discretion thereat having called there

Address confirmation:

☒ **#4 Corporation or Partnership or Trust or LLC**
By delivering thereat a true copy of each to **Joanne Hood** personally. Deponent knew said entity so served to be the entity described in said aforementioned document as said subject and knew said individual to be **Vice President** thereof.

☐ **#5 MAILING**
On , service was completed by mailing a true copy of above document(s) to the above address in a 1st Class postpaid properly addressed envelope marked "Personal and Confidential" from a depository under the exclusive care and custody of the United States Post Office in the State of New York.

☐ An additional mailing was completed to the address above by certified mail.

☒ **#6 DESCRIPTION**
Sex: Female **Color of skin**: Black **Color of hair**: Black **Age**: 25 - 35 Yrs.
Height: 5 ft 5 in - 5 ft 8 in **Weight**: 131-160 Lbs. **Other Features**:

☐ **#7 MILITARY SERVICE**
Deponent asked person spoken to whether the person to be served is currently active in the military service of the United States or of the State of New York, and was informed that said person is not.

☐ **#8 WITNESS FEES**
Subpoena Fee Tendered in the amount of $

☐ **#9 OTHER**

Sworn to before me on December 13, 2024

BRUCE LAZARUS
NOTARY PUBLIC - STATE OF NEW YORK
No. 01LA4992593
Qualified in New York County
My Commission Expires July 12, 2026

Reginald Hunter
1346142

LEGAL EASE INC